

# The Weil group

Enzo Giannotta

February 3, 2024

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Notation</b>	<b>2</b>
<b>3</b>	<b>Unramified extensions</b>	<b>2</b>
<b>4</b>	<b>Tamely ramified extensions</b>	<b>4</b>
<b>5</b>	<b>An example</b>	<b>5</b>
<b>6</b>	<b>The Weil group</b>	<b>6</b>
<b>A</b>	<b>Hensel's Lemma</b>	<b>14</b>
<b>B</b>	<b>The universal property of the projective limit</b>	<b>14</b>

God exists since mathematics is  
consistent, and the Devil exists  
since we cannot prove it.

---

*André Weil*

## 1 Introduction

Given a local field  $F$ , we can consider a separable closure  $F^{\text{sep}}$  of  $F$ . We have already seen that the Galois group  $\text{Gal}(F^{\text{sep}}/F)$  is a *profinite* group with the *krull topology*; we call this group the **absolute Galois group** of  $F$ , and denote it by  $G_F$ . This group encapsulates the arithmetic information of  $F$ , so it is natural for us to study it. A very fruitful technique to study groups is studying its *representations*, i.e., studying group homomorphisms  $G_F \rightarrow \text{Aut}_F(V)$ , where  $V$  is an  $F$ -vector space (not necessarily finite dimensional) and  $\text{Aut}_F(V)$  is its group of  $F$ -automorphisms; typically we take  $F = \mathbb{C}$  and restrict ourselves to *continuous representations*, for example, when  $V$  has  $\dim_{\mathbb{C}}(V) = 1$  we want  $G_F \rightarrow \text{Aut}_{\mathbb{C}}(V) \cong \mathbb{C}^{\times}$  to be continuous with the usual topology on  $\mathbb{C}^{\times}$ ; in this case the image is finite! In other words, we don't have many representations of  $G_F$ . This presents a problem, because having a richer availability of representations would help us understand better the group

$G_F$ ; a solution: constructing a subgroup  $\mathcal{W}_F$  of  $G_F$ , with a topology (different from the subspace topology!) such that it is a locally compact topological group with a neighbourhood basis for the identity made of compact open subgroups (this is called a **locally profinite group**);  $\mathcal{W}_F$  will be called the **Weil group** of  $F$ ; being locally profinite means that we have “more” representations.

## 2 Notation

Let  $L/F$  be an algebraic field extension of a local non-archimedean field  $F$ <sup>1</sup>, such that if  $|\cdot|_v$  is the absolute value of  $F$ , it can be extended uniquely by the absolute value  $|\cdot|_w$  of  $L$ . In this context, let  $\mathcal{O}_F = \{x \in F \mid |x|_v \leq 1\}$  the **valuation ring** of  $F$ ; it has only one non zero prime ideal  $\mathfrak{p}_F = \{x \in F \mid |x|_v < 1\}$ , generated by one element  $\varpi_F$  (it is not unique, nor canonical), named a **uniformizer** of  $F$ . Similarly, we have for  $L$  the objects  $\mathcal{O}_L, \mathfrak{p}_L$  and  $\varpi_L$ . We can form the **residual field** of  $F$ , and similarly of  $L$ , it is the quotient  $\kappa_F = \mathcal{O}_F/\mathfrak{p}_F$ . The inclusion  $\mathcal{O}_F \subset \mathcal{O}_L$  induces an embedding  $\kappa_F \subset \kappa_L$ . Notice that  $\kappa_L/\kappa_F$  is algebraic because  $L/F$  is. By definition of local non-archimedean field, we have that  $\kappa_F$  is a finite field, say  $\mathbb{F}_q$  (in particular,  $F$  is *perfect*); the characteristic of  $\kappa_p$  is a prime  $p > 0$ , called the **residual characteristic** of  $F$ , therefore  $\#\kappa_F = q = p^r$  for some  $r \in \mathbb{N}$ .

When  $L = F^{\text{sep}}$ , we have  $\kappa_L = \bar{\kappa}_F$ , i.e., the *algebraic closure* of  $\kappa_F$ .

## 3 Unramified extensions

**Definition 3.1.** A finite algebraic extension  $L/F$  is said to be **unramified**, if

$$[L : F] = [\kappa_L : \kappa_F].$$

When  $L/F$  is not necessarily finite, we will say that it is **unramified** if it is the union of finite unramified subextensions  $K/F$  of  $L$ .

Consider an automorphism  $\sigma \in \text{Gal}(L/F)$ , then  $\sigma : \mathcal{O}_L \rightarrow \sigma_L$  is well defined and  $\sigma(\mathfrak{p}_L) = \mathfrak{p}_L$ . Therefore, quotient by  $\mathfrak{p}_L$  induces a  $\kappa_F$ -automorphism  $\bar{\sigma} : \kappa_L \rightarrow \kappa_L, \bar{\sigma}([x]) = [\sigma(x)]$  in  $\text{Gal}(\kappa_L/\kappa_F)$ . In other words, we have an homomorphism:

$$\begin{aligned} \text{Gal}(L/F) &\longrightarrow \text{Gal}(\kappa_L/\kappa_F) \\ \sigma &\longmapsto \bar{\sigma}. \end{aligned}$$

In fact, it's not hard to see that it is surjective. In general, when  $L/F$  is not unramified, this map is not injective, however:

**Observation 3.2.** Let  $L/F$  be a finite unramified extension. Then  $\sigma \mapsto \bar{\sigma}$  is an isomorphism between  $\text{Gal}(L/F)$  and  $\text{Gal}(\kappa_L/\kappa_F)$ , because both groups have the same cardinality.

<sup>1</sup>That is,  $F$  is a finite extension of the  $p$ -adic numbers  $\mathbb{Q}_p$  or a finite separable extension of the field of Laurent series  $\mathbb{F}_q((t))$  with variable  $t$  and coefficients in the finite field with  $q = p^r$  elements  $\mathbb{F}_q$ .

**Proposition 3.3.** *Let  $L$  and  $K$  be to algebraic extensions of  $F$ . If  $L/F$  is unramified, then  $LK/K$  is too. If  $L' \subset L$  is a subextension, then  $L'/F$  is unramified.*

*Moreover, if  $L/K$  and  $K/F$  are both algebraic and unramified, then  $L/F$  is algebraic and unramified.*

*Proof.* Without loss of generality we may assume that  $L/F$  is finite. Then  $\kappa_L/\kappa_F$  is also finite, and because it is separable, there exists a primitive element  $\beta = \bar{\alpha} \in \kappa_L$ , with  $\alpha \in \mathcal{O}_L$  and  $\bar{\alpha}$  is its residual class, such that  $\kappa_L = \kappa_F(\beta) = \kappa_F(\bar{\alpha})$ . Let  $f \in \mathcal{O}_F$  be the minimal polynomial of  $\alpha$  over  $F$  and  $\bar{f}(X) \in \kappa_F[X]$  its reduction  $\bmod \mathfrak{p}_F$ . Because

$$[\kappa_L : \kappa_F] \leq \deg \bar{f} = \deg f = [F(\alpha) : F] \leq [L : F] \stackrel{L/F \text{ is unramified}}{=} [\kappa_L : \kappa_F],$$

we can conclude that each inequality is in fact an equality and that  $L = F(\alpha)$  and  $\bar{f}$  is the minimal polynomial of  $\bar{\alpha}$  over  $\kappa_F$ .

Thus, we have  $LK = K(\alpha)$ . So, in order to prove that  $K(\alpha)/K$  is unramified, let  $g \in \mathcal{O}_K$  be the minimal polynomial of  $\alpha$  over  $K$  and  $\bar{g} \in \kappa_K$  its reduction  $\bmod \mathfrak{p}_K$ .  $\bar{g}$  must be irreducible over  $\kappa_K$ , if not, Hensel's Lemma [A](#) would imply that  $g$  is reducible over  $\mathcal{O}_K$ . We obtain:

$$[\kappa_{K(\alpha)} : \kappa_K] \leq [K(\alpha) : K] = \deg g = \deg \bar{g} = [\kappa_K(\bar{\alpha}) : \kappa_K] \leq [\kappa_{K(\alpha)} : \kappa_K].$$

This implies  $[K(\alpha) : K] = [\kappa_{K(\alpha)} : \kappa_K]$ , i.e.,  $K(\alpha)/K$  is unramified.

If  $K/F$  is a subextension of an unramified extension  $L/F$ , then it follows from what we have just proven that  $L/K$  is unramified, hence so is  $K/F$  by the formula for the degree.

Let  $L/K$  and  $K/F$  be two algebraic unramified extensions. Without loss of generality, we may assume that both are finite. Then  $L/F$  is unramified because degrees of field (and residue field) extensions are multiplicative.  $\square$

**Corollary 3.4.** *The composition of two unramified extensions is unramified.*

*Proof.* Without loss of generality, it is enough to show that given to finite unramified extensions  $L/F$  and  $L'/F$ , then  $LL'/F$  is also unramified. Last proposition implies that  $LL'/L'$  is unramified. Also,  $L'/K$  is unramified, then again, by last proposition (last part), we have that  $LL'/F$  is unramified.  $\square$

**Definition 3.5.** Let  $L/F$  be an algebraic extension. Then the composition of all unramified subextensions of  $L$  over  $F$  is again unramified, and it is the unique maximal unramified subextension of  $L$  over  $F$ , denoted by  $L^{\text{ur}} \subset L$ .

In particular, when  $L = F^{\text{sep}}$ , we will write  $F^{\text{ur}}$  instead of  $L^{\text{ur}}$ ; we will simply call it the **maximal unramified extension** of  $F$  (in  $F^{\text{sep}}$ ).

**Proposition 3.6.** *Let  $L/F$  be an algebraic extension. Then*

$$\kappa_{L^{\text{ur}}} = \kappa_L.$$

*In particular, when  $L = F^{\text{sep}}$ , we have*

$$\kappa_{F^{\text{ur}}} = \kappa_{F^{\text{sep}}} = \bar{\kappa}_F.$$

*Proof.* Let  $\bar{\alpha} \in \kappa_L$  with  $(\alpha \in \mathcal{O}_L)$ , we have to show that  $\bar{\alpha} \in \kappa_{L^{\text{ur}}}$ . Let  $\bar{f} \in \kappa_F[X]$  be the minimal polynomial of  $\bar{\alpha}$  in  $\kappa_F$  and  $f \in \mathcal{O}_F[X]$  a monic polynomial such that  $\bar{f} = f \pmod{\mathfrak{p}_F}$ . Then  $f(X)$  must be irreducible because  $\bar{f}$  is, and by Hensel's Lemma [A](#), it has a root  $\alpha$  in  $L$  such that  $\bar{\alpha} \equiv \alpha \pmod{\mathfrak{p}_L}$ , i.e.,  $[F(\alpha) : F] = [\kappa_F(\bar{\alpha}) : \kappa_F]$ . This means that  $F(\alpha)/F$  is unramified, so that  $F(\alpha) \subset L^{\text{ur}}$ , thus  $\bar{\alpha}$  is in fact inside  $\kappa_{F^{\text{ur}}}$ .  $\square$

**Observation 3.7.**  $F^{\text{ur}}$  contains all the roots of unity of order  $m$  coprime to  $p = \text{Char} \kappa_F$  because the separable polynomial  $X^m - 1$  splits completely over  $\bar{\kappa}_F$ , thus over  $F^{\text{ur}}$  thanks to Hensel's Lemma (see the Appendix [A](#)). Because  $\kappa_F$  is finite, the subextensions of  $F^{\text{ur}}/F$  are generated by this roots of unity because  $\bar{\kappa}_F/\kappa_F$  is.

Conversely, if  $L/F$  is a finite unramified extension of degree  $m \geq 1$  with  $L \subset F^{\text{sep}}$ , then in the first paragraph in the proof of Proposition [3.3](#), we actually prove that  $L = F(\alpha)$  for some  $\alpha \in F$  such that its minimal polynomial  $f$  is the lift of the minimal polynomial  $\bar{f}$  of  $\bar{\alpha}$ , and  $\kappa_L = \kappa_F(\bar{\alpha})$ . Because  $\kappa_F$  is a finite field of order  $q$ , and  $\kappa_L/\kappa_F$  is a finite extension of degree  $[L : F] = m$ ,  $\bar{\alpha}$  is a primitive  $(q^m - 1)$ -th root of unity, so is  $\alpha$ .

In summary, there is a 1 – 1 correspondence between finite subextensions of  $F^{\text{ur}}$  over  $F$  of degree  $m \geq 1$  and extensions of  $F$  generated by a primitive  $(q^m - 1)$ -th root of unity, say  $\zeta_{q^m-1}$ , more specifically:  $F(\zeta_{q^m-1})$ .

## 4 Tamely ramified extensions

Now we will weaken the definition of unramified extension and get analogous results as the previous section. The proofs can be found in Chapter II, Section 7 of [\[Neu13\]](#).

**Definition 4.1.** A finite algebraic extension  $L/F$  is said to be **tamely ramified**, if

$$p \nmid [L : L^{\text{ur}}].$$

When  $L/F$  is not necessarily finite, we will say that it is **tamely ramified** if every finite subextension  $L'/L^{\text{ur}}$  has  $p \nmid [L' : L^{\text{ur}}]$ .

**Observation 4.2.** Note that when  $L/F$  is finite, both definitions coincide with the usual ones related to the *ramification index*  $e(L/F)$  of  $F$  over  $L$ :

$$\begin{aligned} L/F \text{ is unramified} &\Leftrightarrow e(L/F) = 1, \\ L/F \text{ is tamely ramified} &\Leftrightarrow p \nmid e(L/F). \end{aligned}$$

**Proposition 4.3.** *Every finite extension  $L/F$  is tamely ramified if and only if  $L/L^{\text{ur}}$  is generated by radicals:*

$$L = L^{\text{ur}}(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}) \quad \text{with } p \nmid m_i.$$

**Corollary 4.4.** *Let  $L$  and  $K$  be to algebraic extensions of  $F$ . If  $L/F$  is tamely ramified, then  $LK/K$  is too. If  $L' \subset L$  is a subextension, then  $L'/F$  is tamely ramified.*

**Corollary 4.5.** *The composition of two tamely ramified extensions is tamely ramified.*

**Definition 4.6.** Let  $L/F$  be an algebraic extension. Then the composition of all tamely ramified subextensions is again tamely ramified, and it is the unique maximal tamely ramified subextension of  $L$  over  $F$ , denoted by  $L^{\text{tr}} \subset L$ .

In particular, when  $L = F^{\text{sep}}$ , we will write  $F^{\text{tr}}$  instead of  $L^{\text{tr}}$ ; we will simply call it the **maximal tamely ramified extension** of  $F$  (in  $F^{\text{sep}}$ ).

**Proposition 4.7.** Let  $L/F$  be an algebraic extension. Then

$$\kappa_{L^{\text{tr}}} = \kappa.$$

In particular, when  $L = F^{\text{sep}}$ , we have  $\kappa_{F^{\text{ur}}} = \bar{\kappa}_F$ .

In summary, we have the following diagram:

$$\begin{array}{ccc} L & & \kappa_L \\ | & & \cup \\ L^{\text{tr}} & & \kappa_L \\ | & & \parallel \\ L^{\text{ur}} & & \kappa_L \\ | & & | \\ \kappa_F & & \kappa_F \end{array}$$

## 5 An example

**Example 5.1.** If  $F = \mathbb{Q}_p$  and  $L = \mathbb{Q}_p(\zeta_n)$ , where  $\zeta_n$  is a primitive  $n$ -th root of unity such that  $n = n'p^m$ ,  $p \nmid n'$ . Then  $L^{\text{ur}} = \mathbb{Q}_p(\zeta_{n'})$  and  $L^{\text{tr}} = L^{\text{ur}}(\zeta_p)$ .

Moreover,  $\mathbb{Q}_p^{\text{ur}} = \mathbb{Q}_p(\zeta_n : p \nmid n)$ , and  $\mathbb{Q}_p^{\text{tr}} = \mathbb{Q}_p^{\text{ur}}(\sqrt[p]{p} : p \nmid m)$ .

In order to give a detailed proof of the example, we will need some previous results:

**Proposition 5.2.** Let  $L := F(\zeta)$ , where  $\zeta$  is a primitive  $n$ -th root of unity. Suppose  $p \nmid n$ . Then, the extension  $L/F$  is unramified of degree  $f$ , where  $f$  is the smallest natural number such that  $q^f \equiv 1 \pmod{n}$ .

*Proof.* If  $\phi(X)$  is the minimal polynomial of  $\zeta$  over  $F$ , then the reduction  $\bar{\phi}(X)$  is the minimal polynomial of  $\bar{\zeta} = \zeta \pmod{\mathfrak{p}_L}$  over  $\kappa_F$ . Indeed, being a divisor of  $X^n - \bar{1}$ ,  $\bar{\phi}$  is separable, and by Hensel's Lemma [A](#) cannot split into factors. Both  $\phi$  and  $\bar{\phi}$  have the same degree, so  $[L : K] = [\kappa_F(\bar{\zeta}) : \kappa] = [\kappa_L : \kappa_F] =: f$ . Therefore,  $L/F$  is unramified. The polynomial  $X^n - 1$  splits over  $\mathcal{O}_L$  and thus (because  $p \nmid n$ ) over  $\kappa_L$  into distinct linear factors, so that  $\kappa_F = \mathbb{F}_{q^f}$  contains the group  $\mu_n$  of  $n$ -th roots of unity and is generated by it. Consequently,  $f$  is the smallest number such that  $\mu_n \subset \mathbb{F}_{q^f}^\times$ , i.e., such that  $n \mid q^f - 1$ .  $\square$

**Proposition 5.3.** Let  $\zeta$  be a primitive  $p^m$ -th root of unity. Then  $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$  is totally ramified of degree  $\varphi(p^m) := (p-1)p^{m-1}$ .

*Proof.* Let  $\xi = \zeta^{p^{m-1}}$ , it is a primitive  $p$ -th root of unity, i.e.,

$$\xi^{p-1} + \xi^{p-2} + \cdots + 1 = 0,$$

hence,

$$\zeta^{(p-1)p^{m-1}} + \zeta^{(p-2)p^{m-1}} + \cdots + 1 = 0.$$

Denote  $\phi(X) := X^{(p-1)p^{m-1}} + X^{(p-2)p^{m-1}} + \cdots + 1$ , then  $\zeta - 1$  is a root of the equation  $\phi(X + 1) = 0$ . But this is irreducible by Eisenstein criterion:  $\phi(1) = p$  and

$$\phi(X) \equiv \frac{X^{p^m-1}}{X^{p^{m-1}}-1} = (X-1)^{p^{m-1}(p-1)} \pmod{p}.$$

It follows that  $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] = \varphi(p^m)$ . □

Now, let's prove the example:

*Proof of the example.* Let  $F = \mathbb{Q}_p$  and  $L = \mathbb{Q}_p(\zeta_n)$  with  $n = n'p^m$  for some  $n'$  coprime with  $p$ . Let  $K := \mathbb{Q}_p(\zeta_{p^m})$ , notice that because  $n'$  and  $p^m$  are coprime, then  $L = K(\zeta_{n'})$ <sup>2</sup>, thus by Proposition 5.2,  $L/K$  is an unramified extension of degree  $f$ , where  $f$  is the smallest number such that  $q_K^f \equiv 1 \pmod{n'}$ , where  $q_K$  is the cardinality of  $\kappa_K$ ; however, by Proposition 5.3,  $K/F$  is *totally ramified*, that means that  $q_L = \#\kappa_L = \#\kappa_F = p$  (in fact, it means that  $[\kappa_L : \kappa_F] = [L : K] = f$ ). In other words,  $f$  is the smallest number such that  $p^f \equiv 1 \pmod{n'}$ . Again, by Proposition 5.2,  $\mathbb{Q}_p(\zeta_{n'})/\mathbb{Q}_p$  is an unramified extension of degree  $f'$ , where  $f'$  is the smallest natural number such that  $p^{f'} \equiv 1 \pmod{n'}$ , i.e.,  $f' = f$ . Finally, to see that  $L^{\text{ur}} = \mathbb{Q}_p(\zeta_{n'})$ , it is enough to show that  $L^{\text{ur}}/F$  has the same index over  $F$  as  $\mathbb{Q}_p(\zeta_{n'})$ . Indeed, by Proposition 3.6,  $[\kappa_{L^{\text{ur}}} : \kappa_F] = [\kappa_L : \kappa_F] = f$ , but  $L^{\text{ur}}/F$  is unramified, so  $[\kappa_{L^{\text{ur}}} : \kappa_L] = [L^{\text{ur}} : F]$ . This concludes that  $\mathbb{Q}_p(\zeta_{n'}) = L^{\text{ur}}$ .

By what we have already discussed and because last proposition says that  $[K : L] = (p-1)p^{m-1}$ , we have  $[L : F] = f(p-1)p^{m-1}$ .

Proposition 5.3, implies that  $F(\zeta_p)$  is tamely ramified because it has degree  $p-1$ , which is coprime to  $p$ ; therefore  $L^{\text{ur}}(\zeta_p) \subset L^{\text{tr}}$ . In order to see that there is in fact equality, notice that  $L^{\text{tr}}/F$  is tamely ramified, in particular  $L^{\text{tr}}/L^{\text{ur}}(\zeta_p)$  too. It divides  $[L : L^{\text{ur}}(\zeta_p)] = p^{m-1}$ . But tamely ramified extensions have degree prime to  $p$  (the characteristic of its residual field), so  $[L^{\text{tr}} : L^{\text{ur}}(\zeta_p)] = 1$ , i.e.  $L^{\text{tr}} = L^{\text{ur}}(\zeta_p)$ .

The last assertion of the example is a particular case of Observation 3.7 and Proposition 4.3. □

## 6 The Weil group

Again we introduce the profinite group with its Krull topology  $G_F := \text{Gal}(F^{\text{sep}}/F)$  with  $F$  a local field; the sets  $\text{Gal}(F^{\text{sep}}/E) \subset G_F$  with  $E/F$  finite and  $E \subset F^{\text{sep}}$  are open. Remember that it is the projective limit  $\varprojlim_E \text{Gal}(E/F)$  over the finite Galois extensions  $E/F$  with  $E \subset F^{\text{sep}}$ .

---

<sup>2</sup>use Bezout's identity:  $\alpha n' + \beta p^m = 1$  for some  $\alpha, \beta \in \mathbb{Z}$ .

**Observation 6.1.** Because  $F^{\text{ur}} = \varinjlim_{E \subset F^{\text{sep}}} E/F$  is the direct limit of the finite unramified extensions  $E/F$  with  $E \subset F^{\text{sep}}$  and taking Galois groups is a contra-variant functor, one can check that

$$\text{Gal}(F^{\text{ur}}/F) = \varprojlim_{E \text{ unramified } /F} \text{Gal}(E/F).$$

*Proof.* Indeed, consider  $H = \text{Gal}(F^{\text{ur}}/F)$  as a topological group with its Krull topology; we have homomorphisms  $\psi_E : H \rightarrow \text{Gal}(E/F), \sigma \mapsto \sigma|_E$  indexed by the pre-ordered (in fact *directed*) set of unramified finite extensions of  $F$  inside  $F^{\text{sep}}$ , ordered by inclusion; more over, they are continuous ( $\text{Gal}(E/F)$  has the discrete topology): let  $\tau \in \text{Gal}(E/F)$  be extended to  $\tilde{\tau} \in \text{Gal}(F^{\text{ur}}/F)$ , then  $\psi_E^{-1}(\tau) = \tilde{\tau} \text{Gal}(F^{\text{ur}}/E)$ , which is a basic open of the Krull topology.

Let  $T_E := \text{Gal}(E/F)$ , we form the projective system  $(T_E, \varphi_{E \subset E'})$ , with the restriction maps  $\varphi_{E \subset E'} : \text{Gal}(E'/F) \rightarrow \text{Gal}(E/F), \sigma \mapsto \sigma|_E$ . Obviously  $(H, \psi_E)$  is compatible with the projective system  $(T_E, \varphi_{E \subset E'})$ , i.e., the next diagram commutes:

$$\begin{array}{ccc} & H & \\ \psi'_E \swarrow & & \searrow \psi_E \\ T_{E'} & \xrightarrow{\varphi_{E \subset E'}} & T_E \end{array}$$

Therefore, by the Universal property of the projective limit **B**, there is a unique map  $\psi : H \rightarrow \varprojlim_{E/F \text{ finite unramified}} T_E$  such that for each  $E/F$  finite unramified, the diagram

$$\begin{array}{ccc} H & \xrightarrow{\psi} & \varprojlim_{E/F \text{ finite unramified}} T_E \\ & \searrow \psi_E & \downarrow p_E \\ & & T_E \end{array}$$

also commutes. Being  $p_E$  the projection to the  $E$ -th coordinate in the Cartesian product  $\prod_{E/F \text{ finite unramified}} \text{Gal}(E/F) \supset \varprojlim_{E/F} T_E$ , the last diagram says that

$$(\psi(\sigma))_E = \sigma|_E, \quad \forall \sigma \in H = \text{Gal}(F^{\text{ur}}/F).$$

Also, it is guaranteed that  $\psi : H \rightarrow \varprojlim_E T_E$  is continuous (see the last part of the Appendix **B**).

Now we show that  $\psi$  is a bijection:

**Injectivity:** Suppose  $\sigma \in H$  is in  $\text{Ker } \psi$ , then for any  $x \in F^{\text{ur}}$ , we have that there is a finite unramified extension  $E$  such that  $x \in E$ , because  $F^{\text{ur}}$  is unramified and by the definition of unramified extension. Then

$$\sigma(x) = (\sigma|_E)(x) = (\psi(\sigma))_E(x) = (p_E(\psi(\sigma)))(x) = x,$$

because  $\psi(\sigma)$  is the identity element in  $\varprojlim_E T_E$ . Because  $x$  was arbitrary, this proves that  $\sigma$  is the identity element in  $H = \text{Gal}(F^{\text{ur}}/F)$ , therefore  $\psi$  is injective.



**Surjectivity:**  $\psi$  is a continuous and  $H$  is compact (it is a profinite group), so the image of  $\psi$  is compact, then is closed because  $\varprojlim_E T_E$  is Hausdorff (it is also a profinite group by definition). Therefore, it is enough show that the image of  $\psi$  is dense to show surjectivity. Indeed, the basic opens in the product topology are of the form

$$\prod_{E \in S} \{\sigma_E\} \times \prod_{E \notin S} T_E,$$

where  $S$  is a finite set of finite unramified extensions  $E/F$ ; because the set of indices are directed by the inclusion, we may assume that  $S$  contains a maximal element  $E'$  such that  $E \subset E'$  is an unramified extension of  $F$  if and only if  $E \in S$ . Therefore, the basic opens of  $\varprojlim_E T_E$  are of the form

$$U_{E'} := \left( \prod_{E \subset E'} \{\tau|_E\} \times \prod_{E \not\subset E'} T_E \right) \cap \varprojlim_E T_E,$$

where  $E'$  is some finite unramified extension of  $F$  and  $\tau \in \text{Gal}(E'/F)$ . Now, clearly any extension  $\tilde{\tau}$  to  $F^{\text{ur}}$  of  $\tau$  satisfies that  $\psi(\tilde{\tau}) \in U_{E'}$ , i.e., the image of  $\psi$  intersects the basic open  $U_{E'}$ . This proves that the image of  $\psi$  is dense, therefore  $\psi$  is surjective.

Finally,  $\psi$  is a closed map because it is continuous with domain a compact space and codomain a Hausdorff space. This show that the bijective continuous map  $\psi$  is in fact an homeomorphism.  $\square$

Because the finite unramified extensions  $E/F$  are in 1 – 1 correspondence with finite extensions over  $\kappa_F$  of degree  $m \geq 1$ , which we know have cyclic Galois group canonically generated by the *Frobenius automorphism*  $x \mapsto x^q$  with  $q = \#\kappa_F$ , we can see that

$$\text{Gal}(F^{\text{ur}}/F) \cong \varprojlim_m \mathbb{Z}/m\mathbb{Z} = \widehat{\mathbb{Z}}.$$

(Remember that the profinite topological group  $\widehat{\mathbb{Z}}$  is the **profinite integers**).

In particular, there exists a unique element  $\Phi_F \in \text{Gal}(F^{\text{ur}}/F)$  which coincides with the inverse of the Frobenius automorphism in each  $\text{Gal}(E/F)$ . We will call it *the geometric Frobenius*.<sup>3</sup> More explicitly, for any finite unramified extension  $E/F$  we have

$$\Phi_F^{-1}(x) \equiv x^q \pmod{\mathfrak{p}_E}, \quad \forall x \in \mathcal{O}_E, \quad (1)$$

where  $q = \#\kappa_F$ , equivalently,

$$\Phi_F(x) \equiv x^{q^{f-1}} \pmod{\mathfrak{p}_E}, \quad \forall x \in \mathcal{O}_E,$$

where  $f = [E : F] = \#\text{Gal}(E/F)$ .

**Definition 6.2.** Lets take the restriction map

$$U : G_F = \text{Gal}(F^{\text{sep}}/F) \longrightarrow \text{Gal}(F^{\text{ur}}/F) \\ \sigma \longmapsto \sigma|_{F^{\text{ur}}}.$$

Then, we say that  $\varphi \in G_F$  is a **geometric Frobenius element** (over  $F$ ), if  $U(\varphi) = \Phi_F$ .

---

<sup>3</sup>We could have chosen  $\Phi_F$  as the unique element which coincides with the Frobenius automorphism in each  $\text{Gal}(E/F)$ , however, we will take the convention of using the geometric Frobenius.



**WARNING 6.3.**  $\varphi$  is not unique! In fact, if we fix a choice  $\varphi_0$  of geometric Frobenius element, then all the other geometric elements are of the form  $\mathcal{I}_F \cdot \varphi_0$ , where  $\mathcal{I}_F := \text{Gal}(F^{\text{sep}}/F^{\text{ur}})$  is the **inertia group** of  $F$ .

Notice that the inertia group  $\mathcal{I}_F$  is a closed subgroup of  $G_F$ , thus it is a profinite group with the subspace topology (which is the Krull topology).

**Proposition 6.4.** *For each  $t \geq 1, p \nmid t$ ,  $F^{\text{ur}}$  has a unique finite extension  $E_t/F^{\text{ur}}$  of degree  $t$ . It is of the form*

$$E_t = F^{\text{ur}}(\sqrt[t]{\varpi_F}).$$

Moreover,

$$\begin{aligned} \text{Gal}(E_t/F^{\text{ur}}) &\longrightarrow \mu_t(F^{\text{ur}}) \\ \sigma &\longmapsto \frac{\sigma(\sqrt[t]{\varpi_F})}{\sqrt[t]{\varpi_F}} \end{aligned}$$

is a canonical isomorphism.<sup>4</sup>

*Proof.* If  $E = F(\sqrt[t]{\varpi_F})$  then  $\varpi := \sqrt[t]{\varpi_F}$  has minimal polynomial  $X^t - \varpi_F$ , which is an Eisenstein polynomial, thus irreducible, so  $E/F$  is a finite extension of degree  $t$ .

Conversely, suppose  $E/F^{\text{ur}}$  is a finite extension of degree  $t$  coprime to  $p$ . By Proposition 3.6,  $t = [E : F^{\text{ur}}] = [\kappa_E, \kappa_{F^{\text{ur}}}]$ , so  $E/F^{\text{ur}}$  is *totally ramified*, this means that  $t = e(E/F^{\text{ur}})$ , i.e.,  $u\varpi_F = \varpi_E^t$  for some unit  $u \in \mathcal{O}_E^\times$  ( $\varpi_F$  is a uniformizer of  $F^{\text{ur}}$  because  $F^{\text{ur}}/F$  is unramified).

Now consider  $f(X) = X^t - u \in \mathcal{O}_E[X]$ , because  $\bar{f} \in \kappa_E[X]$  is separable ( $p \nmid t$ ) and  $\kappa_E = \kappa_{F^{\text{ur}}} = \bar{\kappa}_F$  (Proposition 3.6)  $\bar{f}$  has a root in  $\kappa_E$ , Hensel's Lemma A implies that there is a root  $r$  of  $f$  in  $\mathcal{O}_E$ . Let  $\varpi = \varpi_E/r$ . Then  $|\varpi|_E = 1$ , so it is a uniformizer of  $E$  and  $L = F^{\text{ur}}(\varpi)$ ; also,  $\varpi^t = \varpi_E^t/r^t = \varpi_E^t/u = \varpi_F$ , i.e.,  $L = F^{\text{ur}}(\sqrt[t]{\varpi_F})$  as desired.

To see that  $\sigma \mapsto \frac{\sigma(\sqrt[t]{\varpi_F})}{\sqrt[t]{\varpi_F}}$  is an isomorphism, notice that the right side is a group of cardinality  $t = [E_t : F^{\text{ur}}] = \# \text{Gal}(E_t/F^{\text{ur}})$  because  $X^t - 1$  has all its roots in  $F^{\text{ur}}$ : indeed, the polynomial  $X^t - \bar{1}$  is separable and has all of its roots in  $\bar{\kappa}_F = \kappa_{F^{\text{ur}}}$  which can be lifted by Hensel's Lemma A to roots in  $F^{\text{ur}}$ . Therefore it is enough to show that this morphism is injective, which is immediate by what we have just already proven:  $E_t$  is generated by  $\sqrt[t]{\varpi_F}$  over  $F^{\text{ur}}$ . Finally, notice that the morphism is well defined:  $\frac{\sigma(\sqrt[t]{\varpi_F})}{\sqrt[t]{\varpi_F}}$  is a root of  $X^t - 1$ .  $\square$

**Observation 6.5.** Because  $F^{\text{tr}} = \varinjlim_E E/F^{\text{ur}}$  is the direct limit of the finite extensions  $E/F^{\text{ur}}$  with degree coprime to  $p$  and  $E \subset F^{\text{sep}}$ , then taking Galois, one can easily check that

$$\text{Gal}(F^{\text{tr}}/F^{\text{ur}}) = \varprojlim_{t \text{ coprime to } p} \text{Gal}(E_t/F^{\text{ur}}) \cong \varprojlim_{p \nmid t} \mu_t(F^{\text{ur}}),$$

in virtue of the previous proposition. More over, this implies

$$\text{Gal}(F^{\text{tr}}/F^{\text{ur}}) \cong \varprojlim_{\ell \neq p} \mathbb{Z}_\ell,$$

where  $\mathbb{Z}_\ell$  are the  $\ell$ -adic integers.

<sup>4</sup>In general,  $\mu_t(K)$  denotes the multiplicative group of  $t$ -th roots of unity in field  $K$ . If  $p$  denotes the characteristic of  $K$ , when  $p \nmid t$  and  $K$  contains all the roots of  $X^t - 1$ , then  $\mu_t(K) \cong \mathbb{Z}/t\mathbb{Z}$ . This happens in our case  $K = F^{\text{ur}}$ .

*Proof.* The proof is completely analogous to that of Observation 6.1.  $\square$

**Definition 6.6.** We write  $\mathcal{P}_F := \text{Gal}(F^{\text{sep}}/F^{\text{tr}})$  for the **wild inertia group** of  $F$ . Notice that unramified extensions are tamely ramified, thus  $F^{\text{ur}} \subset F^{\text{tr}}$ , and then  $\mathcal{P}_F \subset \mathcal{I}_F$ .

Notice that the wild inertia group  $\mathcal{P}_F$  of  $F$  is a closed subgroup of  $G_F$ , thus it is a profinite group with the subspace topology (which is the krull topology).

**Proposition 6.7.** *The group  $\mathcal{P}_F$  is a pro- $p$ -group.*

*Proof.* Indeed,  $\mathcal{P}_F$  is a projective limit of finite  $p$ -groups:

$$\mathcal{P}_F = \varprojlim_{p \nmid t} \text{Gal}(E_t/F^{\text{ur}}),$$

and Proposition 6.4 says that  $\text{Gal}(E_t/F^{\text{ur}}) \cong \mu_t(F^{\text{ur}}) \cong \mathbb{Z}/t\mathbb{Z}$ . Therefore  $\mathcal{P}_F$  is a pro- $p$ -group by definition (see [RV98]).  $\square$

**Proposition 6.8.**  *$\mathcal{P}_F$  is the unique  $p$ -Sylow subgroup of  $\mathcal{I}_F$ .*

*Proof.* In order to see that  $\mathcal{P}_F$  is the unique  $p$ -Sylow subgroup of  $\mathcal{I}_F$ , it is enough to show that  $\mathcal{P}_F \triangleleft \mathcal{I}_F$  and that  $[\mathcal{I}_F : \mathcal{P}_F]$  is coprime with  $p$  as a supernatural number. Indeed,  $\mathcal{P}_F$  is normal in  $G_F$  because  $F^{\text{tr}}/F$  is Galois, and  $[\mathcal{I}_F : \mathcal{P}_F]$  is coprime with  $p$  because  $\mathcal{I}_F/\mathcal{P}_F$  is the projective limit  $\varprojlim_{\ell \neq p} \mathbb{Z}_\ell$  of pro- $\ell$ -groups with  $\ell \neq p$ .  $\square$

**Definition 6.9.** The **Weil group**  $\mathcal{W}_F$ , at least algebraically, is the subgroup of  $G_F$  defined as the inverse image of  $U^{-1}(\langle \Phi_F \rangle)$ . In other words,

$$\mathcal{W}_F = \mathcal{I}_F \cdot \langle \varphi \rangle,$$

where  $\varphi$  is a Frobenius element (notice that  $\mathcal{W}_F$  doesn't depend on the choice of  $\varphi$ ).

Observe that  $\mathcal{W}_F$  is the semi-direct product of  $\mathcal{I}_F$  and  $\langle \varphi \rangle$ :  $\mathcal{I}_F$  is normal because is the kernel of the map  $U$ , and  $\mathcal{I}_F \cap \langle \varphi \rangle = \{1\}$ . In particular every element  $\sigma \in \mathcal{W}_F$  can be uniquely written as  $\sigma = i\varphi^n$  for some  $i \in \mathcal{I}_F$  and  $n \in \mathbb{Z}$ .

**Proposition 6.10.** *The Weil group has the following properties:*

1.  $\mathcal{W}_F$  is dense in  $G_F$ .
2.  $\mathcal{W}_F \triangleleft G_F$ .
3. Because  $\mathcal{W}_F$  is a group, to define a topology in  $\mathcal{W}_F$ , it is enough to define a neighbourhood basis for the identity of  $\mathcal{W}_F$ : these open sets will be those of  $\mathcal{I}_F$  in its subspace topology respect to  $G_F$ .

Whats more, this topology makes  $\mathcal{W}_F$  a locally profinite group, and the inclusion  $\iota_F : \mathcal{W}_F \hookrightarrow G_F$  is continuous.

4. We have a continuous homomorphism

$$\begin{aligned} \|\cdot\|_F : \mathcal{W}_F &\longrightarrow \mathbb{Q}^\times \subset \mathbb{R}^\times \\ \sigma &\longmapsto \|\sigma\|_F := q^{-v_F(\sigma)}, \end{aligned}$$

where  $v_F(\sigma)$  denotes the integer  $n$  such that  $U(\sigma) = \Phi_F^n$ .

*Proof.* In what follows, we will identify  $\widehat{\mathbb{Z}}$  with  $\text{Gal}(F^{\text{ur}}/F)$  and  $\mathbb{Z}$  with  $\mathcal{W}_F$  via  $U$ .

(a) Let  $\sigma \in G_F$ . Then  $U(\sigma) \in \widehat{\mathbb{Z}}$  has an element of  $\mathbb{Z}$  arbitrarily near because  $\mathbb{Z} \subset \widehat{\mathbb{Z}}$  is dense. By basic properties of the Krull topology, to show that  $\mathcal{W}_F$  is dense in  $G_F$ , it is enough to show that there is an element of  $\mathcal{W}_F$  inside  $\sigma \text{Gal}(F^{\text{sep}}/E)$  for any finite Galois extension  $E/F$ . But  $U(\text{Gal}(F^{\text{sep}}/E)) = \text{Gal}(F^{\text{ur}}/E \cap F^{\text{ur}}) = \text{Gal}(F^{\text{ur}}/E^{\text{ur}})$ ; this last group is open in the Krull topology because  $E^{\text{ur}}/F$  is a finite extension, thus it contains an element of  $\mathbb{Z}$ . Taking preimage, we see that  $\sigma \text{Gal}(F^{\text{sep}}/E)$  contains an element of  $\mathcal{W}_F$ . This proves the first assertion.

(b) Obvious:  $\mathcal{W}_F = U^{-1}(\mathbb{Z})$  and  $\mathbb{Z}$  is normal in  $\widehat{\mathbb{Z}}$ .

(c) Notice that around each element  $x = i\varphi^n \in \mathcal{W}_F$  with  $i \in \mathcal{I}_F$  a neighbourhood basis for  $x$  is  $\{U \cdot \varphi^n\}_U$  with  $U$  ranging over the open sets around  $i$  in the subspace topology of  $\mathcal{I}_F$ .

First, it is a topological group because the map

$$\begin{aligned} \mathcal{W}_F \times \mathcal{W}_F &\longrightarrow \mathcal{W}_F \\ (x, y) &\longmapsto xy^{-1} \end{aligned}$$

is continuous, indeed, if  $x = i\varphi^n$  with  $i \in \mathcal{I}_F$  and  $y = j\varphi^m$  with  $j \in \mathcal{I}_F$  and

$$xy^{-1} = i\varphi^n \varphi^{-m} j^{-1} = i\varphi^{n-m} j^{-1} = i(\varphi^{n-m} j^{-1} \varphi^{m-n}) \varphi^{n-m},$$

then it is enough to check that there are open subsets of  $\mathcal{I}_F$ , say  $U$  and  $V$ , such that  $(U\varphi^n) \cdot (V\varphi^m) \subset W \cdot \varphi^{n-m}$  for any  $W \ni i(\varphi^{n-m} j^{-1} \varphi^{m-n})$  open subset of  $\mathcal{I}_F$ . Indeed, we can find such  $U$  and  $V$  because the map

$$\begin{aligned} \mathcal{I}_F \times \mathcal{I}_F &\longrightarrow \mathcal{I}_F \\ (i, j) &\longmapsto i\varphi^{n-m} j^{-1} \varphi^{m-n} \end{aligned}$$

is continuous for any  $n, m \in \mathbb{Z}$  fixed.

It is locally compact because any  $x = i\varphi^n \in \mathcal{W}_F$  is in the open compact neighbourhood  $\mathcal{I}_F \varphi^n$ : the topology that we gave  $\mathcal{W}_F$  was so that  $\mathcal{I}_F$  is a topological subspace, and  $\mathcal{I}_F$  has the induced topology of the profinite group  $G_F$ , thus  $\mathcal{I}_F$  is also compact because it is closed in  $G_F$ ; by construction of  $\mathcal{W}_F$ ,  $\mathcal{I}_F$  is open. What is more, a basis of open subgroups of  $\mathcal{I}_F$  form a neighbourhood basis of the identity in  $\mathcal{W}_F$ ; open subgroups in topological groups are closed, therefore these open subgroups are compact in the subspace topology of  $\mathcal{I}_F$ , because  $\mathcal{I}_F$  is. This proves that  $\mathcal{W}_F$  is locally profinite.

Notice that the map  $v_F : \mathcal{W}_F \rightarrow \mathbb{Z}, i\varphi^n \mapsto n$  is continuous with the discrete topology of  $\mathbb{Z}$ . Also, if we identify  $\widehat{\mathbb{Z}}$  with  $\text{Gal}(F^{\text{ur}}/F)$ , we have that the subspace

topology of  $\mathbb{Z}$  in  $\widehat{\mathbb{Z}}$  is the discrete topology. Finally, to see that  $\iota_F : \mathcal{W}_F \hookrightarrow G_F$  is continuous, let  $\sigma \text{ Gal}(F^{\text{sep}}/E)$  be a basic open set in  $G_F$  with  $E/F$  finite Galois extension, then  $U(\sigma \text{ Gal}(F^{\text{sep}}/E)) = \sigma|_{F^{\text{ur}}} \text{ Gal}(F^{\text{ur}}/E^{\text{ur}})$  is open in  $\text{Gal}(F^{\text{ur}}/F)$ , thus identifying it with  $\widehat{\mathbb{Z}}$ , we have that  $\mathcal{W}_F \cap \iota_F^{-1}(\sigma \text{ Gal}(F^{\text{sep}}/E))$  corresponds via the continuous map  $\mathcal{W}_F \rightarrow \mathbb{Z}$  with the preimage of  $\sigma|_{F^{\text{ur}}} \text{ Gal}(F^{\text{ur}}/E^{\text{ur}}) \cap \mathbb{Z}$ , therefore it is open.

- (d) In the last paragraph we have seen that  $v_F : \mathcal{W}_F \rightarrow \mathbb{Z}$  is continuous ( $\mathbb{Z}$  has the discrete topology). The map  $\mathbb{Z} \rightarrow \mathbb{R}^\times, n \mapsto q^{-n}$  is again continuous, therefore the composition  $\|\cdot\|_F : \sigma \mapsto q^{-v_F(\sigma)}$  is continuous.

□

**Remark 6.11.**

1.  $\mathcal{W}_F$  doesn't have the subspace topology in  $G_F$ , indeed, if so  $\mathcal{J}_F$  would be open in  $G_F$ , thus of finite index ( $G_F$  is compact), however, it is not the case:  $U$  has infinite image.
2.  $\mathcal{J}_F$  is a maximal compact subgroup of  $\mathcal{W}_F$ , indeed,  $\mathcal{W}_F/\mathcal{J}_F$  is isomorphic to  $\mathbb{Z}$  as a discrete topological group (by last paragraph of item (c) the homeomorphism is induced by  $v_F : \mathcal{W}_F \rightarrow \mathbb{Z}$ ), so if there was a compact subgroup  $W \subset \mathcal{W}_F$  such that  $W \supsetneq \mathcal{J}_F$ , then it would be mapped to a nontrivial compact subgroup of  $\mathbb{Z}$ , thus finite because  $\mathbb{Z}$  is discrete, but  $\mathbb{Z}$  doesn't have non trivial finite subgroups.

**Proposition 6.12.** *Let  $E/F$  be a finite extension with  $E \subset F^{\text{sep}}$ . Then  $G_E \hookrightarrow G_F$  induces a homeomorphism*

$$\mathcal{W}_E \xrightarrow{\sim} \mathcal{W}_F \cap G_E =: \mathcal{W}_F^E.$$

*whats more,  $\mathcal{W}_F^E$  is an open subgroup of finite index in  $\mathcal{W}_F$ , and it is normal if and only if  $E/F$  is Galois; when this happens,  $\mathcal{W}_F/\mathcal{W}_F^E \cong G_F/G_E \cong \text{Gal}(E/F)$ . Conversely, if  $W$  is a open subgroup of finite index of  $\mathcal{W}_F$ , then  $W = \mathcal{W}_F^E$  for some finite extension  $E/F$  with  $E \subset F^{\text{sep}}$ .*

*Proof.* Obviously it is a bijection.

Now, let  $f = f(E/F)$  be the residual degree of  $E$  over  $F$ . We have that  $f = [\kappa_E : \kappa_F]$ , thus Frobenius elements in  $G_E$  correspond with  $f$ -powers of Frobenius elements in  $G_F$ . Therefore, we can see that basic open sets from both sides correspond to open sets in the other side. This proves that is a homeomorphism.

The map of homogeneous spaces  $\mathcal{W}_F/\mathcal{W}_F^E \rightarrow G_F/G_E$  induced by taking quotients is injective, and by density of the Weil group it is surjective, so it is a bijection. The fact that  $\mathcal{W}_F^E$  is open in  $\mathcal{W}_F$  comes from the continuity of  $\iota_F$ , and that it has finite index is due to the beginning of this paragraph:  $[\mathcal{W}_F : \mathcal{W}_F^E] = [G_F : G_E] = [E : F] < +\infty$ . If  $E/F$  is Galois,  $G_E \triangleleft G_F$ , then  $\mathcal{W}_F^E \triangleleft \mathcal{W}_F$ . Conversely, is  $\mathcal{W}_F^E \triangleleft \mathcal{W}_F$  then  $G_E \triangleleft G_F$  by density, i.e.,  $E/F$  is Galois.

Let  $W \subset \mathcal{W}_F$  be an open subgroup of finite index. Let  $I = \mathcal{J}_F \cap W$ ; it is an open subgroup (therefore also closed) of  $\mathcal{J}_F$ , then by compactness of  $\mathcal{J}_F$ , we have that  $I$  has finite index  $t$  in  $\mathcal{J}_F$ . Because  $\mathcal{J}_F = \text{Gal}(F^{\text{sep}}/F^{\text{ur}})$ , Galois correspondence

implies that there exists a finite extension  $E$  of  $F^{\text{ur}}$ , such that  $I = \text{Gal}(F^{\text{sep}}/E)$ . Let  $\varphi_F \in \text{Gal}(F^{\text{ur}}/F)$  be the geometric Frobenius, write  $E = F^{\text{ur}}(\alpha)$  for some primitive element  $\alpha \in E$ , we can extend  $\varphi_F$  as the identity on  $\alpha$ , and then extend it again as an element of  $\text{Gal}(F^{\text{sep}}/F)$ ; by construction, it will be a geometric Frobenius element  $\varphi \in G_F$ , such that  $\varphi(\alpha) = \alpha$ .

Now, because  $W$  has finite index in  $\mathcal{W}_F$ , there is an integers  $r \geq 1$ , such that  $\varphi \in W$ . Let  $n$  be the minimum integer such that  $i\varphi^n \in W$ , for some  $i \in \mathcal{I}_F$ . We affirm that  $W = I \cdot \langle \varphi^n \rangle$ . The inclusion  $\supset$  is clear. For the converse, let  $\sigma = i\varphi^j$  with  $i \in \mathcal{I}_F$ ; write  $j = qn + s$ , then  $i\varphi^s = \sigma(\varphi^n)^{-q} \in W$ , so by minimality of  $n$ ,  $s = 0$  and  $n \mid j$ , i.e.  $\varphi^j \in \langle \varphi^n \rangle$ ; in particular,  $i = \sigma(\varphi^n)^{-q} \in W$  so  $i \in W \cap \mathcal{I}_F = I$ . This proves the other inclusion  $\subset$ .

Finally, let  $L \subset F^{\text{ur}}$  be an unramified extension of  $F$  of degree  $n$ . We will prove that  $W = \mathcal{W}_F^T = \mathcal{W}_F \cap G_T$ , where  $T := L(\alpha)$  (Notice that  $T/F$  is finite). Indeed, first we will show that  $W \subset G_T$ , then we will show that  $[\mathcal{W}_F : W] \leq [\mathcal{W}_F : \mathcal{W}_F \cap G_T]$ :

1. For this, it is enough to show that if  $x \in L$  and  $y = \alpha$  then  $\sigma(x) = x$  and  $\sigma(y) = y$  for all  $\sigma \in W$ . Because  $W = I \langle \varphi^n \rangle$ , it is enough to show this for  $\sigma \in I = \text{Gal}(F^{\text{sep}}/F^{\text{ur}}(\alpha))$  and  $\sigma = \varphi^n$ . First, suppose  $\sigma \in I$ :

$$\sigma(x) = x \text{ because } x \in L \subset F^{\text{ur}},$$

and

$$\sigma(y) = y \text{ because } I = \text{Gal}(F^{\text{sep}}/F^{\text{ur}}(\alpha)).$$

Then, suppose  $\sigma = \varphi^n$ , on one hand,  $L/F$  is an unramified extension of degree  $n$ , and because  $\varphi^{-n}$  acts as  $z \mapsto z^{q^n} \equiv z \pmod{\mathfrak{p}_L}$  (see (1)), i.e. the identity automorphism in  $\text{Gal}(\kappa_L/\kappa_F)$  and the map  $\text{Gal}(L/F) \rightarrow \text{Gal}(\kappa_L/\kappa_L)$  is an isomorphism because  $L/F$  is unramified (see Observation 3.2), we have that  $\varphi^{-n}$  restricted to  $L$  is the trivial automorphism, so  $\varphi^n$  too, therefore

$$\sigma(x) = x.$$

On the other hand, we chose at the beginning  $\varphi$  such that  $\varphi(\alpha) = \alpha$ , in other words:

$$\varphi(y) = y, \text{ therefore } \sigma(y) = y.$$

2. Lets compute  $[\mathcal{W}_F, \mathcal{W}_F^T]$ , by what we have already proven,

$$[\mathcal{W}_F, \mathcal{W}_F^T] = [G_F : G_T] = [T : F] = [L(\alpha) : L][L : F] \geq t[L : F] = tn.$$

But

$$[\mathcal{W}_F : W] = [\mathcal{W}_F : I \langle \varphi^n \rangle] = [\mathcal{I}_F : I][\langle \varphi \rangle : \langle \varphi^n \rangle] = [E : F^{\text{ur}}]n = tn.$$

Therefore  $[\mathcal{W}_F : W] \leq [\mathcal{W}_F, \mathcal{W}_F^T]$ , so  $W = \mathcal{W}_F^T$ .

□

## A Hensel's Lemma

Let  $F$  be a *complete* field with respect to a non-archimedean absolute value  $|\cdot|_v$  (for example if  $F$  is a local non-archimedean field). We will say that a polynomial  $f \in \mathcal{O}_F[X]$  is **primitive**, if its reduction  $\bmod \mathfrak{p}_F$  in  $\kappa_F[X]$  is not the zero polynomial, i.e.

$$\max\{|a_0|_v, \dots, |a_n|_v\} = 1,$$

where  $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathcal{O}_F[X]$ .

**Theorem A.1** (Hensel's Lemma). *If a primitive polynomial  $f \in \mathcal{O}_F[X]$  admits a  $\bmod \mathfrak{p}_F$  factorization*

$$f(X) \equiv \bar{g}(X)\bar{h}(X) \pmod{\mathfrak{p}_F}$$

*into relatively prime polynomials  $\bar{g}, \bar{h} \in \kappa_F[X]$ , then  $f$  admits a factorization*

$$f(X) = g(X)h(X)$$

*into polynomials  $g, h \in \mathcal{O}_F[X]$  such that  $\deg(g) = \deg(\bar{g})$  and*

$$g(X) \equiv \bar{g}(X) \pmod{\mathfrak{p}_F} \quad \text{and} \quad h(X) \equiv \bar{h}(X) \pmod{\mathfrak{p}_F}.$$

*Proof.* See [Neu13][Hensel's Lemma (4.6)]. □

**Remark A.2.** We cannot guarantee that the degree of  $g$  and  $h$  coincide with the degree of  $\bar{g}$  and  $\bar{h}$ , respectively, at the same time because the degree of  $f$  may diminish when taking  $\bmod \mathfrak{p}_F$ : being primitive doesn't imply that the principal coefficient of  $f$  is not divisible by  $\mathfrak{p}_F$ . However, if we assume that the principal coefficient of  $f$  is not divisible by  $\mathfrak{p}_F$ , i.e. it is in  $\mathcal{O}_F^\times$  (for example when  $f$  is monic), we can deduce that if  $\deg g = \deg \bar{g}$ , then from

$$\deg g + \deg h = \deg f = \deg \bar{f} = \deg \bar{g} + \deg \bar{h}$$

we have  $\deg h = \deg \bar{h}$ .

## B The universal property of the projective limit

Let  $I$  be a preordered set of indices and let  $\{G_i\}_{i \in I}$  be a family of sets. Assume further that for every pair of indices  $i, j \in I$  with  $i \leq j$ , we have an associated mapping  $\varphi_{ij} : G_j \rightarrow G_i$ , subject to the following conditions:

- (i)  $\varphi_{ii} = \text{Id}_{G_i}$  for all  $i \in I$ .
- (ii)  $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$  for all  $i \leq j \leq k$  in  $I$ .

Then the system  $(G_i, \varphi_{ij})$  is called a **projective** (or **inverse**) system.

**Definition B.1.** Let  $(G_i, \varphi_{ij})$  be a projective system of sets. Then we define the **projective limit** (or **inverse limit**) of the system, denoted by  $\varprojlim_i G_i$ , by

$$\varprojlim_i G_i = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid i \leq j \Rightarrow \varphi_{ij}(g_j) = g_i \right\}.$$

Note that  $\varprojlim_i G_i$  is a subset of the direct product  $\prod_{i \in I} G_i$ , thus it comes equipped with projection maps  $p_j : \varprojlim_i G_i \rightarrow G_j$  for all  $j \in I$ . Furthermore, we have the next *universal property*:

**Theorem B.2** (Universal property of the projective limit). *Let  $H$  be a nonempty set together with maps  $\psi_i : H \rightarrow G_i$  for all  $i \in I$  such that they are compatible with the projective system  $(G_i, \varphi_{ij})$ , more precisely, for each pair  $i, j \in I$  with  $i \leq j$ , the following diagram commutes:*

$$\begin{array}{ccc} & H & \\ \swarrow \psi_j & & \searrow \psi_i \\ G_j & \xrightarrow{\varphi_{ij}} & G_i \end{array}$$

*Then there exists a unique map  $\psi : H \rightarrow \varprojlim_i G_i$  such that for each  $i \in I$  the diagram*

$$\begin{array}{ccc} H & \xrightarrow{\psi} & \varprojlim_i G_i \\ & \searrow \psi_i & \downarrow p_i \\ & & G_i \end{array}$$

*also commutes.*

This construction was done in the category of sets, but replacing the inverse system  $(G_i, \varphi_{ij})$  with topological groups and morphisms  $\varphi_{ij}$  of topological groups, and giving  $\varprojlim_i G_i \subset \prod_{i \in I} G_i$  the subspace topology of the product topology results in a topological group in its own right, enjoying the same universal property as before, but where the set  $H$  is a topological group and all the maps are morphisms in the category of topological groups.



## References

- [Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
- [RV98] Dinakar Ramakrishnan and Robert J Valenza. *Fourier analysis on number fields*, volume 186. Springer Science & Business Media, 1998.