The Weil group

Enzo Giannotta

March 26, 2024

Contents

> 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^{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 $G_F \to \text{Aut}_F(V)$, 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 $G_F \to \text{Aut}_{\mathbb{C}}(V) \cong \mathbb{C}^\times$ 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 $\mathscr{W}_F$ 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**); $\mathscr{W}_F$ 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[1], 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 $\mathscr{O}_F = \{x \in F \mid |x|_v \leqslant 1\}$ 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 ϖ_F (it is not unique, nor canonical), named *a* **uniformizer** of F. Similarly, we have for L the objects $\mathscr{O}_L, \mathfrak{p}_L$ and ϖ_L. We can form the **residual field** of F, and similarly of L, it is the quotient $\kappa_F = \mathscr{O}_F/\mathfrak{p}_F$. The inclusion $\mathscr{O}_F \subset \mathscr{O}_L$ induces an embedding $\kappa_F \subset \kappa_L$. Notice that κ_L/κ_F is algebraic because L/F is. By definition of local non-archimedean field, we have that κ_F is a finite field, say $\mathbb{F}_q$ (in particular, F is *perfect*); the characteristic of κ_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 $L = F^{\mathrm{sep}}$, we have $\kappa_L = \overline{\kappa}_F$, i.e., the *algebraic closure* of κ_F.

3 Unramified extensions

Definition 3.1. — A <u>finite</u> 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 $\sigma \in \mathrm{Gal}(L/F)$, then $\sigma : \mathscr{O}_L \to \sigma_L$ is well defined and $\sigma(\mathfrak{p}_L) = \mathfrak{p}_L$. Therefore, quotient by $\mathfrak{p}_L$ induces a κ_F-automorphism $\overline{\sigma} : \kappa_L \to \kappa_L, \overline{\sigma}([x]) = [\sigma(x)]$ in $\mathrm{Gal}(\kappa_L/\kappa_F)$. In other words, we have an homomorphism:

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

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 $\sigma \mapsto \overline{\sigma}$ is an isomorphism between $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(\kappa_L/\kappa_F)$, because both groups have the same cardinality.

[1] 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 κ_L/κ_F is also finite, and because it is separable, there exists a primitive element $\beta = \overline{\alpha} \in \kappa_L$, with $\alpha \in \mathcal{O}_L$ and $\overline{\alpha}$ is its residual class, such that $\kappa_L = \kappa_F(\beta) = \kappa_F(\overline{\alpha})$. Let $f \in \mathcal{O}_F$ be the minimal polynomial of α over F and $\overline{f}(X) \in \kappa_F[X]$ its reduction $\mod \mathfrak{p}_F$. Because

$$[\kappa_L : \kappa_F] \leqslant \deg \overline{f} = \deg f = [F(\alpha):F] \leqslant [L:F] \overset{L/F \text{ is unramified}}{=} [\kappa_L : \kappa_F],$$

we can conclude that each inequality is in fact an equality and that $L = F(\alpha)$ and $\overline{f}$ is the minimal polynomial of $\overline{\alpha}$ over κ_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 α over K and $\overline{g} \in \kappa_K$ its reduction $\mod \mathfrak{p}_K$. $\overline{g}$ must be irreducible over κ_K, if not, Hensel's Lemma A would imply that g is reducible over $\mathcal{O}_K$. We obtain:

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

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. □

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. □

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 $L^{\mathrm{ur}} \subset L$.

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

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

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

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

$$\kappa_{F^{\mathrm{ur}}} = \kappa_{F^{\mathrm{sep}}} = \overline{\kappa}_F.$$

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

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

Conversely, if L/F is a finite unramified extension of degree $m \geqslant 1$ with $L \subset F^{\mathrm{sep}}$, 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 $\overline{f}$ of $\overline{\alpha}$, and $\kappa_L = \kappa_F(\overline{\alpha})$. Because κ_F is a finite field of order q, and κ_L/κ_F is a finite extension of degree $[L:F] = m$, $\overline{\alpha}$ is a primitive $(q^m - 1)$-th root of unity, so is α.

In summary, there is a $1-1$ correspondence between finite subextensions of F^{ur} over F of degree $m \geqslant 1$ and extensions of F generated by a primitive $(q^m - 1)$-th root of unity, say ζ_{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 <u>finite</u> algebraic extension L/F is said to be **tamely ramified**, if

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

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

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:

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

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

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

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 $L^{\mathrm{tr}} \subset L$.

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

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

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

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

In summary, we have the following diagram:

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

5 An example

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

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

Proposition 5.2. — *Let $L := F(\zeta)$, where ζ 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 $q^f \equiv 1 \mod n$.*

Proof. If $\phi(X)$ is the minimal polynomial of ζ over F, then the reduction $\overline{\phi}(X)$ is the minimal polynomial of $\overline{\zeta} = \zeta \mod \mathfrak{p}_L$ over κ_F. Indeed, being a divisor of $X^n - \overline{1}$, $\overline{\phi}$ is separable, and by Hensel's Lemma A cannot split into factors. Both ϕ and $\overline{\phi}$ have the same degree, so $[L : K] = [\kappa_F(\overline{\zeta}) : \kappa] = [\kappa_L : \kappa_F] =: f$. Therefore, L/F is unramified. The polynomial $X^n - 1$ splits over $\mathcal{O}_L$ and thus (because $p \nmid n$) over κ_L into distinct linear factors, so that $\kappa_F = \mathbb{F}_{q^f}$ contains the group μ_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 $n \mid q^f - 1$. □

Proposition 5.3. — *Let ζ 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

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

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

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 $L = K(\zeta_{n'})$[2], thus by Proposition 5.2, L/K is an unramified extension of degree f, where f is the smallest number such that $q_K^f \equiv 1 \mod n'$, where q_K is the cardinality of κ_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 $p^f \equiv 1 \mod n'$. 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 $p^{f'} \equiv 1 \mod n'$, i.e., $f' = f$. Finally, to see that $L^{\mathrm{ur}} = \mathbb{Q}_p(\zeta_{n'})$, it is enough to show that L^{ur}/F has the same index over F as $\mathbb{Q}_p(\zeta_{n'})$. Indeed, by Proposition 3.6, $[\kappa_{L^{\mathrm{ur}}} : \kappa_F] = [\kappa_L : \kappa_F] = f$, but L^{ur}/F is unramified, so $[\kappa_{L^{\mathrm{ur}}} : \kappa_L] = [L^{\mathrm{ur}} : F]$. This concludes that $\mathbb{Q}_p(\zeta_{n'}) = L^{\mathrm{ur}}$.

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

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

6 The Weil group

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

Observation 6.1. — Because $F^{\mathrm{ur}} = \lim_{E \longrightarrow} E/F$ is the direct limit of the finite unramified extensions E/F with $E \subset F^{\mathrm{sep}}$ and taking Galois groups is a contravariant functor, one can check that

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

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

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

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

$$\begin{tikzcd} & H \arrow[dl, "\psi'_E"'] \arrow[dr, "\psi_E"] & \\ T_{E'} \arrow[rr, "\varphi_{E\subset E'}"'] & & T_E \end{tikzcd}$$

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

$$\begin{tikzcd} H \arrow[r, "\psi"] \arrow[dr, "\psi_E"'] & \varprojlim_{E/F \text{ finite unramified}} T_E \arrow[d, "p_E"] \\ & T_E \end{tikzcd}$$

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

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

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

Now we show that ψ is a bijection:

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

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

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

Surjectivity: ψ is a continuous and H is compact (it is a profinite group), so the image of ψ 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 ψ 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 $\tau \in \mathrm{Gal}(E'/F)$. Now, clearly any extension $\widetilde{\tau}$ to F^{ur} of τ satisfies that $\psi(\widetilde{\tau}) \in U_{E'}$, i.e., the image of ψ intersects the basic open $U_{E'}$. This proves that the image of ψ is dense, therefore ψ is surjective.

Finally, ψ 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 ψ is in fact an homeomorphism. □

Because the finite unramified extensions E/F are in $1-1$ correspondence with finite extensions over κ_F of degree $m \geqslant 1$, 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

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

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

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

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

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

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

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

Definition 6.2. — Lets take the restriction map

$$\begin{aligned} U : G_F = \mathrm{Gal}(F^{\mathrm{sep}}/F) &\longrightarrow \mathrm{Gal}(F^{\mathrm{ur}}/F) \\ \sigma &\longmapsto \sigma\big|_{F^{\mathrm{ur}}}. \end{aligned}$$

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

WARNING 6.3. — φ is not unique! In fact, if we fix a choice φ_0 of geometric Frobenius element, then all the other geometric elements are of the form $\mathscr{I}_F \cdot \varphi_0$, where $\mathscr{I}_F := \mathrm{Gal}(F^{\mathrm{sep}}/F^{\mathrm{ur}})$ is the **inertia group** of F.

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

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

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

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

Moreover,

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

is a canonical isomorphism.[4]

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

Now consider $f(X) = X^t - u \in \mathscr{O}_E[X]$, because $\overline{f} \in \kappa_E[X]$ is separable ($p \nmid t$) and $\kappa_E = \kappa_{F^{\mathrm{ur}}} = \overline{\kappa}_F$ (Proposition 3.6) $\overline{f}$ has a root in κ_E, Hensel's Lemma A implies that there is a root r of f in $\mathscr{O}_E$. Let $\varpi = \varpi_E/r$. Then $|\varpi|_E = 1$, so it is an uniformizer of E and $L = F^{\mathrm{ur}}(\varpi)$; also, $\varpi^t = \varpi_E^t/r^t = \varpi_E^t/u = \varpi_F$, i.e., $L = F^{\mathrm{ur}}(\sqrt[t]{\varpi_F})$ 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 $t = [E_t : F^{\mathrm{ur}}] = \#\mathrm{Gal}(E_t/F^{\mathrm{ur}})$ because $X^t - 1$ has all its roots in F^{ur}: indeed, the polynomial $X^t - \overline{1}$ is separable and has all of its roots in $\overline{\kappa}_F = \kappa_{F^{\mathrm{ur}}}$ which can be lifted by Hensel's Lemma A to roots in F^{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^{ur}. Finally, notice that the morphism is well defined: $\frac{\sigma(\sqrt[t]{\varpi_F})}{\sqrt[t]{\varpi_F}}$ is a root of $X^t - 1$. □

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

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

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

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

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

Proof. The proof is completely analogous to that of Observation 6.1. □

[4] 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 $K = F^{\mathrm{ur}}$).

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

Notice that the wild inertia group $\mathscr{P}_F$ 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 $\mathscr{P}_F$ is a pro-p-group.*

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

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

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

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

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

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

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

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

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

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

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

   Whats more, this topology makes $\mathscr{W}_F$ a locally profinite group, and the inclusion $\iota_F : \mathscr{W}_F \hookrightarrow G_F$ is continuous.
4. *We have a continuous homomorphism*

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

   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 $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ and $\mathbb{Z}$ with $\mathscr{W}_F$ 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 $\mathscr{W}_F$ is dense in G_F, it is enough to show that there is an element of $\mathscr{W}_F$ inside $\sigma\,\mathrm{Gal}(F^{\mathrm{sep}}/E)$ for any finite Galois extension E/F. But $U(\mathrm{Gal}(F^{\mathrm{sep}}/E)) = \mathrm{Gal}(F^{\mathrm{ur}}/E \cap F^{\mathrm{ur}}) = \mathrm{Gal}(F^{\mathrm{ur}}/E^{\mathrm{ur}})$; this last group is open in the Krull topology because E^{ur}/F is a finite extension, thus it contains an element of $\mathbb{Z}$. Taking preimage, we see that $\sigma\,\mathrm{Gal}(F^{\mathrm{sep}}/E)$ contains an element of $\mathscr{W}_F$. This proves the first assertion.

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

(c) Notice that around each element $x = i\varphi^n \in \mathscr{W}_F$ with $i \in \mathscr{I}_F$ 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 $\mathscr{I}_F$.

First, it is a topological group because the map

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

is continuous, indeed, if $x = i\varphi^n$ with $i \in \mathscr{I}_F$ and $y = j\varphi^m$ with $j \in \mathscr{I}_F$ 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 $\mathscr{I}_F$, 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 $\mathscr{I}_F$. Indeed, we can find such U and V because the map

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

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

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

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

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

$\square$

Remark 6.11. —

1. $\mathscr{W}_F$ doesn't have the subspace topology in G_F, indeed, if so $\mathscr{I}_F$ 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. $\mathscr{I}_F$ is a maximal compact subgroup of $\mathscr{W}_F$, indeed, $\mathscr{W}_F/\mathscr{I}_F$ is isomorphic to $\mathbb{Z}$ as a discrete topological group (by last paragraph of item (c) the homeomorphism is induced by $v_F : \mathscr{W}_F \to \mathbb{Z}$), so if there was a compact subgroup $W \subset \mathscr{W}_F$ such that $W \supsetneq \mathscr{I}_F$, 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*

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

whats more, $\mathscr{W}_F^E$ is an open subgroup of finite index in $\mathscr{W}_F$, and it is normal if and only if E/F is Galois; when this happens, $\mathscr{W}_F/\mathscr{W}_F^E \cong G_F/G_E \cong \mathrm{Gal}(E/F)$. Conversely, if W is a open subgroup of finite index of $\mathscr{W}_F$, then $W = \mathscr{W}_F^E$ 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 $\mathscr{W}_F/\mathscr{W}_F^E \to G_F/G_E$ induced by taking quotients is injective, and by density of the Weil group it is surjective, so it is a bijection. The fact that $\mathscr{W}_F^E$ is open in $\mathscr{W}_F$ comes from the continuity of ι_F, and that it has finite index is due to the beginning of this paragraph: $[\mathscr{W}_F : \mathscr{W}_F^E] = [G_F : G_E] = [E : F] < +\infty$. If E/F is Galois, $G_E \lhd G_F$, then $\mathscr{W}_F^E \lhd \mathscr{W}_F$. Conversely, is $\mathscr{W}_F^E \lhd \mathscr{W}_F$ then $G_E \lhd G_F$ by density, i.e., E/F is Galois.

Let $W \subset \mathscr{W}_F$ be an open subgroup of finite index. Let $I = \mathscr{I}_F \cap W$; it is an open subgroup (therefore also closed) of $\mathscr{I}_F$, then by compactness of $\mathscr{I}_F$, we have that I has finite index t in $\mathscr{I}_F$. Because $\mathscr{I}_F = \mathrm{Gal}(F^{\text{sep}}/F^{\text{ur}})$, Galois correspondence implies that there exists a finite extension E of F^{ur}, such that $I = \mathrm{Gal}(F^{\text{sep}}/E)$. Let $\varphi_F \in \mathrm{Gal}(F^{\text{ur}}/F)$ be the geometric Frobenius, write $E = F^{\text{ur}}(\alpha)$ for some primitive element $\alpha \in E$, we can extend φ_F as the identity on α, and then extend it again as an element of $\mathrm{Gal}(F^{\text{sep}}/F)$; 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 $\mathscr{W}_F$, there is an integers $r \geqslant 1$, such that $\varphi \in W$. Let n be the minimum integer such that $i\varphi^n \in W$, for some $i \in \mathscr{I}_F$. We affirm that $W = I \cdot \langle \varphi^n \rangle$. The inclusion $\supset$ is clear. For the converse, let $\sigma = i\varphi^j$ with $i \in \mathscr{I}_F$; 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 $i \in W \cap \mathscr{I}_F = I$. This proves the other inclusion $\subset$.

Finally, let $L \subset F^{\mathrm{ur}}$ be an unramified extension of F of degree n. We will prove that $W = \mathscr{W}_F^T = \mathscr{W}_F \cap G_T$, 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 $[\mathscr{W}_F : W] \leqslant [\mathscr{W}_F : \mathscr{W}_F \cap G_T]$:

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 $\sigma \in I = \mathrm{Gal}(F^{\mathrm{sep}}/F^{\mathrm{ur}}(\alpha))$ and $\sigma = \varphi^n$. First, suppose $\sigma \in I$:

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

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

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

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

   On the other hand, we chose at the beginning φ such that $\varphi(\alpha) = \alpha$, in other words:
$$\varphi(y) = y, \text{ therefore } \sigma(y) = y.$$

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

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

   But

$$[\mathscr{W}_F : W] = [\mathscr{W}_F : I\langle \varphi^n \rangle] = [\mathscr{I}_F : I][\langle \varphi \rangle : \langle \varphi^n \rangle] = [E : F^{\mathrm{ur}}]n = tn.$$
   Therefore $[\mathscr{W}_F : W] \leqslant [\mathscr{W}_F, \mathscr{W}_F^T]$, so $W = \mathscr{W}_F^T$.

□

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 $\mod \mathfrak{p}_F$ in $\kappa_F[X]$ is not the zero polynomial, i.e.

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

where $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathcal{O}_F[X]$.

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

$$f(X) \equiv \overline{g}(X)\overline{h}(X) \mod \mathfrak{p}_F$$

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

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

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

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

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 $\overline{g}$ and $\overline{h}$, respectively, at the same time because the degree of f may diminish when taking $\mod \mathfrak{p}_F$: 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 $\deg g = \deg \overline{g}$, then from

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

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

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 $i \leqslant j$, we have an associated mapping $\varphi_{ij} : G_j \to G_i$, subject to the following conditions:

(i) $\varphi_{ii} = \mathrm{Id}_{G_i}$ for all $i \in I$.

(ii) $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ for all $i \leqslant j \leqslant k$ in I.

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

Definition B.1. — Let (G_i, φ_{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

$$\varprojlim_i G_i := \left\{ (g_i)_i \in \prod_{i \in I} G_i \;\middle|\; i \leqslant j \Rightarrow \varphi_{ij}(g_j) = g_i \right\}.$$

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 $p_j : \varprojlim_i G_i \to G_j$ 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 $\psi_i : H \to G_i$ for all $i \in I$ such that they are compatible with the projective system (G_i, φ_{ij}), more precisely, for each pair $i, j \in I$ with $i \leqslant j$, the following diagram commutes:*

$$\begin{tikzcd} & H \arrow[dl, "\psi_j"'] \arrow[dr, "\psi_i"] & \\ G_j \arrow[rr, "\varphi_{ij}"] & & G_i \end{tikzcd}$$

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

$$\begin{tikzcd} H \arrow[r, "\psi"] \arrow[dr, "\psi_i"'] & \varprojlim_i G_i \arrow[d, "p_i"] \\ & G_i \end{tikzcd}$$

also commutes.

This construction was done in the category of sets, but replacing the inverse system (G_i, φ_{ij}) with topological groups and morphisms φ_{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.