Chapter 7

$\mathfrak{p}$-adic fields

In this chapter, we study completions of number fields, and their ramification (in particular in the Galois case). We then look at extensions of the p-adic numbers $\mathbb{Q}_p$ and classify them through their ramification, though they are actually completion of number fields. We will address again the question of ramification in number fields, and see how ramification locally can help us to understand ramification globally.

By $\mathfrak{p}$-adic fields, we mean, in modern terminology, local fields of characteristic zero.

Definition 7.1. Let K be a number field, and let $\mathfrak{p}$ be a prime. Let ν be the place associated with $\mathfrak{p}$ and $|\cdot|_\nu = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_\mathfrak{p}(\cdot)}$ (recall that a place is an equivalence class of absolute values, inside which we take as representative the normalized absolute value). We set K_ν or $K_\mathfrak{p}$ the completion of K with respect to the $|\cdot|_\nu$-adic topology. The field K_ν admits an absolute value, still denoted by $|\cdot|_\nu$, which extends the one of K.

In other words, we can also define K_ν as

$$K_\nu = \frac{\{(x_n) \mid (x_n) \text{ is a Cauchy sequence with respect to } |\cdot|_\nu\}}{\{(x_n) \mid x_n \to 0\}}.$$

This is a well defined quotient ring, since the set of Cauchy sequence has a ring structure, and those which tend to zero form a maximal ideal inside this ring. Intuitively, this quotient is here to get the property that all Cauchy sequences whose terms get closer and closer to each other have the same limit (and thus define the same element in K_ν).

Example 7.1. The completion of $\mathbb{Q}$ with respect to the induced topology by $|\cdot|_p$ is $\mathbb{Q}_p$.

Below is an example with an infinite prime.

Example 7.2. If ν is a real place, then $K_\nu = \mathbb{R}$. If ν is a complex place, then $K_\nu = \mathbb{C}$.

Let us now compute an example where K is not $\mathbb{Q}$.

Example 7.3. Let $K = \mathbb{Q}(\sqrt{7})$. We want to compute its completion K_ν where ν is a place above 3. Since

$$3\mathcal{O}_K = (-2-\sqrt{7})(-2+\sqrt{7}),$$

there are two places ν_1, ν_2 above 3, corresponding to the two finite primes

$$\mathfrak{p}_1 = (-2-\sqrt{7})\mathcal{O}_K,\ \mathfrak{p}_2 = (-2+\sqrt{7})\mathcal{O}_K.$$

Now the completion K_ν where ν is one of the ν_i, $i = 1, 2$, is an extension of $\mathbb{Q}_3$, since the ν_i-adic topology on K extends the 3-adic topology on $\mathbb{Q}$.

Since $K = \mathbb{Q}[X]/(X^2 - 7)$, we have that K contains a solution for the equation $X^2 - 7$. We now look at this equation in $\mathbb{Q}_3$, and similarly to what we have computed in Example 5.3, we have that a solution is given by

$$1 + 3 + 3^2 + 2 \cdot 3^4 + \dots$$

Thus

$$K_\nu \simeq \mathbb{Q}_3.$$

One can actually show that the two places correspond to two embeddings of K into $\mathbb{Q}_3$.

In the following, we consider only finite places. Let ν be a finite place of a number field.

Definition 7.2. We define the integers of K_ν by

$$\mathcal{O}_\nu = \{x \in K_\nu \mid |x|_\nu \leq 1\}.$$

The definition of absolute value implies that $\mathcal{O}_\nu$ is a ring, and that

$$\mathfrak{m}_\nu = \{x \in K_\nu \mid |x|_\nu < 1\}$$

is its unique maximal ideal (an element of $\mathcal{O}_\nu$ not in $\mathfrak{m}_\nu$ is a unit of $\mathcal{O}_\nu$). Such a ring is called a local ring.

Example 7.4. The ring of integers $\mathcal{O}_\nu$ of $K_\nu = \mathbb{Q}_p$ is $\mathbb{Z}_p$, and $\mathfrak{m}_\nu = p\mathbb{Z}_p$.

We have the following diagram

$$\begin{array}{ccc} K & \xrightarrow{dense} & K_\nu \\ | & & | \\ \mathcal{O}_K & \xrightarrow{dense} & \mathcal{O}_\nu \\ | & & | \\ \mathfrak{p} & \xrightarrow{dense} & \mathfrak{m}_\nu \end{array}$$

We already have the notion of residue field for $\mathfrak{p}$, given by

$$\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}.$$

We can similarly define a residue field for $\mathfrak{m}_\nu$ by

$$\mathbb{F}_\nu = \mathcal{O}_\nu/\mathfrak{m}_\nu.$$

We can prove that

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathcal{O}_\nu/\mathfrak{m}_\nu.$$

7.1 Hensel's way of writing

Let π_ν be in $\mathfrak{m}_\nu$ but not in $\mathfrak{m}_\nu^2$, so that $\mathrm{ord}_{\mathfrak{m}_\nu}(\pi_\nu) = 1$. We call π_ν a uniformizer of $\mathfrak{m}_\nu$ (or of $\mathcal{O}_\nu$). For example, for $\mathbb{Z}_p$, we can take $\pi = p$. We now choose a system of representatives of $\mathcal{O}_\nu/\mathfrak{m}_\nu$:

$$\mathcal{C} = \{c_0 = 0, c_1, \ldots, c_{q-1}\},$$

where $q = |\mathbb{F}_{\mathfrak{p}}| = \mathrm{N}(\mathfrak{p})$. For example, for $\mathbb{Z}_p$, we have $\mathcal{C} = \{0, 1, 2, \ldots, p-1\}$. The set

$$\{\pi_\nu^k c_0, \pi_\nu^k c_1, \ldots, \pi_\nu^k c_{q-1}\} = \pi_\nu^k \mathcal{C}$$

is a system of representatives for $\mathfrak{m}_\nu^k/\mathfrak{m}_\nu^{k+1}$.

Lemma 7.1. *1. Every element $\alpha \in \mathcal{O}_\nu$ can be written in a unique way as*

$$\alpha = a_0 + a_1\pi_\nu + a_2\pi_\nu^2 + \ldots$$

with $a_i \in \mathcal{C}$.

2. An element of $\alpha \in K_\nu$ can be written as

$$\alpha = a_{-k}\pi_\nu^{-k} + a_{-k+1}\pi_\nu^{-k+1} + \ldots.$$

3. The uniformizer generates the ideal $\mathfrak{m}_\nu$, that is

$$\pi_\nu^k \mathcal{O}_\nu = \mathfrak{m}_\nu^k.$$

4. $|\alpha|_\nu = |\mathbb{F}_\nu|^{-k}$, where $\alpha = a_k\pi_\nu^k + \ldots$, $a_k \neq 0$.

Proof. 1. Let $\alpha \in \mathcal{O}_\nu$. Let $a_0 \in \mathcal{C}$ be the representative of the class $\alpha + \mathfrak{m}_\nu$ in $\mathcal{O}_\nu/\mathfrak{m}_\nu$. We set

$$\alpha_1 = \frac{\alpha - a_0}{\pi_\nu}.$$

We have that $\alpha_1 \in \mathcal{O}_\nu$, since

$$|\alpha_1|_\nu = \frac{|\alpha - a_0|_\nu}{|\pi_\nu|_\nu} \leq 1.$$

Indeed, $a_0 \in \alpha + \mathfrak{m}_\nu$ implies that $\alpha - a_0 \in \mathfrak{m}_\nu$ and thus $|\alpha - a_0|_\nu \leq |\pi_\nu|_\nu$. By replacing α by α_1, we find $a_1 \in \mathcal{C}$ such that

$$\alpha_2 = \frac{\alpha_1 - a_1}{\pi_\nu} \in \mathcal{O}_\nu.$$

By iterating this process k times, we get

$$\begin{aligned} \alpha &= a_0 + \alpha_1 \pi_\nu \\ &= a_0 + a_1 \pi_\nu + \alpha_2 \pi_\nu^2 \\ &\vdots \\ &= a_0 + a_1 \pi_\nu + a_2 \pi_\nu^2 + \ldots + \alpha_{k+1} \pi_\nu^{k+1}. \end{aligned}$$

Thus

$$|\alpha - (a_0 + a_1 \pi_\nu + a_2 \pi_\nu^2 + \ldots + a_k \pi_\nu^k)|_\nu = |\alpha_{k+1}|_\nu |\pi_\nu|_\nu^{k+1} \to 0$$

when $k \to \infty$, since $\pi_\nu \in \mathfrak{m}_\nu$ and thus by definition of $\mathfrak{m}_\nu$, $|\pi_\nu|_\nu < 1$.

2. We multiply $\alpha \in K_\nu$ by $\pi_\nu^{-\mathrm{ord}_{\mathfrak{m}_\nu}(\alpha)}$, so that

$$\pi_\nu^{-\mathrm{ord}_{\mathfrak{m}_\nu}(\alpha)} \alpha \in \mathcal{O}_\nu$$

and we conclude by 1.

3. It is clear that

$$\pi_\nu^k \mathcal{O}_\nu \subset \mathfrak{m}_\nu^k.$$

Conversely, let us take $\alpha \in \mathfrak{m}_\nu^k$. We then have that

$$a_0 = a_1 = \ldots = a_{k-1} = 0$$

and thus

$$\alpha = a_k \pi_\nu^k + \ldots \in \pi_\nu^k \mathcal{O}_\nu.$$

4. Since $\alpha = a_k \pi_\nu^k + \ldots$, $a_k \neq 0$, we have that $\alpha \in \pi_\nu^k \mathcal{O}_\nu = \mathfrak{m}_\nu^k$ but not in $\mathfrak{m}_\nu^{k+1}$, and

$$\alpha \in \pi_\nu^k \mathcal{O}_\nu^\times.$$

Thus

$$|\alpha|_\nu = |\pi_\nu|_\nu^k.$$

Now note that if π_ν and π'_ν are two uniformizers, then $|\pi_\nu| = |\pi'_\nu|$, and thus, we could have taken a uniformizer in the number field rather than in its completion, that is, $\pi'_\nu \in \mathfrak{p}$ but not in $\mathfrak{p}^2$, which yields

$$|\pi'_\nu| = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\pi'_\nu)} = \mathrm{N}(\mathfrak{p})^{-1} = |\mathbb{F}_\mathfrak{p}|^{-1} = |\mathbb{F}_\nu|^{-1}.$$

□

7.2 Hensel's Lemmas

Lemma 7.2. (First Hensel's Lemma). *Let $f(X) \in \mathcal{O}_\nu[X]$ be a monic polynomial, and let $\tilde{f}(X) \in \mathbb{F}_\nu[X]$ be the reduction of f modulo $\mathfrak{m}_\nu$. Let us assume that there exist two coprime monic polynomials ϕ_1 and ϕ_2 in $\mathbb{F}_\nu[X]$ such that*

$$\tilde{f} = \phi_1\phi_2.$$

Then there exists two monic polynomials f_1 and f_2 in $\mathcal{O}_\nu[X]$ such that

$$f = f_1 f_2,\ \tilde{f}_1 = \phi_1,\ \tilde{f}_2 = \phi_2.$$

Proof. We first prove by induction that we can construct polynomials $f_1^{(k)}, f_2^{(k)}$ in $\mathcal{O}_\nu[X]$, $k \geq 1$, such that

$$\begin{array}{lll} (1) & f & \equiv f_1^{(k)} f_2^{(k)} \mod \mathfrak{m}_\nu^k \\ (2) & f_i^{(k)} & \equiv f_i^{(k-1)} \mod \mathfrak{m}_\nu^{k-1}. \end{array}$$

(k=1). Since we know by assumption that there exist ϕ_1, ϕ_2 such that $\tilde{f} = \phi_1\phi_2$, we lift ϕ_i in a monic polynomial $f_i^{(1)} \in \mathcal{O}_\nu[X]$, and we have $\deg f_i^{(1)} = \deg \phi_i$.

(True up to k). We have already built $f_i^{(k)}$. Using the condition (1), there exists a polynomial $g \in \mathcal{O}_\nu[X]$ such that

$$f = f_1^{(k)} f_2(k) + \pi_\nu^k g.$$

Using Bézout's identity for the ring $\mathbb{F}_\nu[X]$, there exists polynomials ψ_1 and ψ_2 in $\mathbb{F}_\nu[X]$ such that

$$\tilde{g} = \phi_1\psi_1 + \phi_2\psi_2$$

since ϕ_1 and ϕ_2 are coprime. We now lift ψ_i in a polynomial $h_i \in \mathcal{O}_\nu[X]$ of same degree, and set

$$f_i^{(k+1)} = f_i^{(k)} + \pi_\nu^k h_i.$$

We now need to check that (1) and (2) are satisfied. (2) is clearly satisfied by construction. Let us check (1). We have

$$\begin{array}{rcl} f_1^{(k+1)} f_2^{(k+1)} & = & (f_1^{(k)} + \pi_\nu^k h_1)(f_2^{(k)} + \pi_\nu^k h_2) \\ & = & f_1^{(k)} f_2^{(k)} + \pi_\nu^k (f_1^{(k)} h_2 + f_2^{(k)} h_1) + \pi_\nu^{2k} h_1 h_2 \\ & \equiv & (f - \pi_\nu^k g) + \pi_\nu^k (f_1^{(k)} h_2 + f_2^{(k)} h_1) \mod \mathfrak{m}_\nu^{k+1}. \end{array}$$

We are now left to show that

$$\pi_\nu^k(-g + f_1^{(k)} h_2 + f_2^{(k)} h_1) \equiv 0 \mod \mathfrak{m}_\nu^{k+1},$$

that is

$$-g + f_1^{(k)} h_2 + f_2^{(k)} h_1 \equiv 0 \mod \mathfrak{m}_\nu$$

or again in other words, after reduction $\mod \mathfrak{m}_\nu$

$$-\tilde{g} + \tilde{f}_1^{(k)}\tilde{h}_2 + \tilde{f}_2^{(k)}\tilde{h}_1 \equiv 0,$$

which is satisfied by construction of h_1 and h_2. So this concludes the proof by induction.

Let us know conclude the proof of the lemma. We set

$$f_i = \lim_{k\to\infty} f_i^{(k)}$$

which converges by (2). By (1) we have that

$$f_1 f_2 = \lim_{k\to\infty} f_1^{(k)} f_2^{(k)} = f.$$

□

Example 7.5. The polynomial $f(X) = X^2 - 2 \in \mathbb{Z}_7[X]$ is factorized as

$$\phi_1 = (X - 3),\ \phi_2 = (X - 4)$$

in $\mathbb{F}_7[X]$.

Corollary 7.3. *Let K be a number field, ν be a finite place of K, and K_ν be its completion. Denote $q = |\mathbb{F}_\nu|$. Then the set μ_{q-1} of $(q-1)$th roots of unity belongs to $\mathcal{O}_\nu$.*

Proof. Let us look at the polynomial $X^{q-1} - 1$. On the finite field $\mathbb{F}_\nu$ with q elements, this polynomial splits into linear factors, and all its roots are exactly all the invertible elements of $\mathbb{F}_\nu$. By Hensel's lemma, $f \in \mathcal{O}_\nu[X]$ can be completely factorized. That is, it has exactly $q - 1$ roots in $\mathcal{O}_\nu$. More precisely, we can write

$$X^{q-1} - 1 = \prod_{\zeta\in\mu_{q-1}} (X - \zeta) \in \mathcal{O}_\nu[X].$$

□

Of course, one can rewrite that μ_{q-1} belongs to $\mathcal{O}_\nu^\times$ since roots of unity are clearly invertible in $\mathcal{O}_\nu$.

Lemma 7.4. (Second Hensel's Lemma). *Let f be a monic polynomial in $\mathcal{O}_\nu[X]$ and let f' be its formal derivative. We assume that there exists $\alpha \in \mathcal{O}_\nu$ such that*

$$|f(\alpha)|_\nu < |f'(\alpha)|_\nu^2.$$

Then there exists $\beta \in \mathcal{O}_\nu$ such that

$$f(\beta) = 0$$

and

$$|\beta - \alpha|_\nu \le \frac{|f(\alpha)|_\nu}{|f'(\alpha)|_\nu} < |f'(\alpha)|_\nu.$$

Proof. We set

$$\begin{aligned} \alpha_0 &= \alpha \\ \alpha_{n+1} &= \alpha_n - \beta_n \end{aligned}$$

where

$$\beta_n = \frac{f(\alpha_n)}{f'(\alpha_n)}.$$

(First part of the proof.) We first show by induction that

1. $|f(\alpha_n)|_\nu < |f(\alpha_{n-1})|_\nu$
2. $|f'(\alpha_n)|_\nu = |f'(\alpha)|_\nu$.

Let us assume these are true for $n \geq 1$, and show they still hold for $n+1$.

Let us first note that

$$\begin{aligned} |\beta_n|_\nu &= \frac{|f(\alpha_n)|_\nu}{|f'(\alpha_n)|_\nu} \\ &< \frac{|f(\alpha)|_\nu}{|f'(\alpha_n)|_\nu} \quad \text{by 1.} \\ &= \frac{|f(\alpha)|_\nu}{|f'(\alpha)|_\nu} \quad \text{by 2.} \\ &< |f'(\alpha)|_\nu \quad \text{by assumption.} \end{aligned}$$

Since $f \in \mathcal{O}_\nu[X]$ and $\alpha \in \mathcal{O}_\nu$, this means that $|f'(\alpha)|_\nu \leq 1$, and in particular implies that $\beta_n \in \mathcal{O}_\nu$.

Let us write $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$, so that

$$\begin{aligned} f(X+\alpha_n) &= a_0 + a_1(X+\alpha_n) + a_2(X^2 + 2X\alpha_n + \alpha_n^2) + \ldots + a_n(X^n + \ldots + \alpha_n^n) \\ &= (a_0 + a_1\alpha_n + a_2\alpha_n^2 + \ldots + a_n\alpha_n^n) + X(a_1 + a_2 2\alpha_n + \ldots + a_n n\alpha_n^{n-1}) + X^2 g(X) \\ &= f(\alpha_n) + f'(\alpha_n)X + g(X)X^2 \end{aligned}$$

with $g(X) \in \mathcal{O}_\nu[X]$. We are now ready to prove that the two properties are satisfied.

1. Let us first check that $|f(\alpha_{n+1})|_\nu < |f(\alpha_n)|_\nu$. We have that

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n - \beta_n) \\ &= f(\alpha_n) + f'(\alpha_n)(-\beta_n) + g(-\beta_n)\beta_n^2 \quad \text{take } X = -\beta_n \\ &= g(-\beta_n)\beta_n^2 \quad \text{recall the definition of} \beta \end{aligned}$$

Let us now consider its absolute value

$$\begin{aligned} |f(\alpha_{n+1})|_\nu &= |g(-\beta_n)|_\nu |\beta_n|_\nu^2 \\ &\leq |\beta_n|_\nu^2 \quad \beta_n \in \mathcal{O}_\nu,\ g \in \mathcal{O}_\nu[X] \\ &< |f(\alpha_n)|_\nu \frac{|f(\alpha)|_\nu}{|f'(\alpha)|_\nu^2} \quad \text{by 1. and 2.} \\ &< |f(\alpha_n)|_\nu \quad \text{by assumption} \end{aligned}$$

2. We now need to prove that $|f'(\alpha_{n+1})|_\nu = |f'(\alpha)|_\nu$. We have that

$$\begin{aligned} |f'(\alpha_{n+1})|_\nu &= |f'(\alpha_n - \beta_n)|_\nu \\ &= |f'(\alpha_n) - \beta_n h(-\beta_n)|_\nu \qquad \text{take again } X = -\beta_n \\ &\leq \max\{|f'(\alpha_n)|_\nu, |\beta_n|_\nu |h(-\beta_n)_\nu|\} \\ &= \max\{|f'(\alpha)|_\nu, |\beta_n|_\nu |h(-\beta_n)_\nu|\} \qquad \text{by 2.} \end{aligned}$$

and equality holds if the two arguments of the maximum are distinct. Now the first argument is $|f'(\alpha)|_\nu$, while the second is

$$\begin{aligned} |\beta_n|_\nu |h(-\beta_n)_\nu| &\leq |\beta_n|_\nu \quad h(-\beta_n) \in \mathcal{O}_\nu \\ &< |f'(\alpha)|_\nu, \end{aligned}$$

which completes the first part of the proof.

(Second part of the proof.) We are now ready to prove that there exists an element $\beta \in \mathcal{O}_\nu$ which satisfies the claimed properties. We set

$$\beta = \lim_{n\to\infty} \alpha_n.$$

Note that this sequence converges, since this is a Cauchy sequence. Indeed, for $n > m$, we have

$$\begin{aligned} |\alpha_n - \alpha_m|_\nu &\leq \max\{|\alpha_n - \alpha_{n-1}|_\nu, \ldots, |\alpha_{m+1} - \alpha_m|_\nu\} \\ &= \max\{|\beta_{n-1}|, \ldots, |\beta_m|_\nu\} \\ &= \frac{1}{|f'(\alpha)|_\nu} \max\{|f(\alpha_{n-1})|_\nu, \ldots, |f(\alpha_m)|_\nu\} \qquad \text{by first part of the proof, part 2.} \\ &= \frac{|f(\alpha_m)|_\nu}{|f'(\alpha)|_\nu} \qquad \text{by first part of the proof, part 1.} \end{aligned}$$

which tends to zero by 1. Let us check that β as defined above satisfies the required properties. First, we have that

$$f(\beta) = f(\lim_{n\to\infty} \alpha_n) = \lim_{n\to\infty} f(\alpha_n) = 0.$$

Since $\mathcal{O}_\nu$ is closed, $\beta \in \mathcal{O}_\nu$, and we have that

$$\begin{aligned} |\beta - \alpha|_\nu &= \lim_{n\to\infty} |\alpha_n - \alpha|_\nu \\ &\leq \lim_{n\to\infty} \max\{|\alpha_n - \alpha_{n-1}|_\nu, \ldots, |\alpha_1 - \alpha|_\nu\} \\ &= \max\{|\beta_{n-1}|, \ldots, |\beta_0|_\nu\} \\ &\leq \frac{|f(\alpha)|_\nu}{|f'(\alpha)|_\nu} \\ &< |f'(\alpha)|_\nu. \end{aligned}$$

□

7.3 Ramification Theory

Let L/K be a number field extension. Let $\mathfrak{P}$ and $\mathfrak{p}$ be primes of L and K respectively, with $\mathfrak{P}$ above $\mathfrak{p}$. Since finite places correspond to primes, $\mathfrak{P}$ and $\mathfrak{p}$ each induce a place (respectively w and v) such that the restriction of w to K coincides with v, that is

$$(|\cdot|_w)_K = |\cdot|_v.$$

This in turn corresponds to a field extension L_w/K_v. We can consider the corresponding residue class fields:

$$\begin{aligned} \mathbb{F}_{\mathfrak{P}} &= \mathcal{O}_L/\mathfrak{P} \simeq \mathcal{O}_w/\mathfrak{m}_w = \mathbb{F}_w \\ \mathbb{F}_{\mathfrak{p}} &= \mathcal{O}_K/\mathfrak{p} \simeq \mathcal{O}_v/\mathfrak{m}_v = \mathbb{F}_v \end{aligned}$$

and we have a finite field extension $\mathbb{F}_w/\mathbb{F}_v$ of degree $f = f_{\mathfrak{P}/|\mathfrak{p}} = f_{w|v}$. Note that this means that the inertial degree f is the same for a prime in L/K and the completion L_w/K_v with respect to this prime.

Lemma 7.5. *Let π_v be a uniformizer of K_v. Then*

$$|\pi_v|_w = |\pi_w|_w^e$$

where $e = e_{\mathfrak{P}/|\mathfrak{p}} = e_{w|v}$ is the ramification index.

Note that this can be rewritten as $\mathfrak{m}_v\mathcal{O}_w = \mathfrak{m}_w^e$, which looks more like the original definition of ramification index.

Proof. We can take $\pi_v \in K$ and $\pi_w \in L$. Then $\pi_v \in \mathfrak{p}$ but not in $\mathfrak{p}^2$, and $\pi_w \in \mathfrak{P}$ but not in $\mathfrak{P}^2$. Thus $\pi_v\mathcal{O}_K = \mathfrak{p}I$ where I is an ideal coprime to $\mathfrak{p}$. If we lift $\mathfrak{p}$ and π_v in $\mathcal{O}_L$, we get

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}},\ \pi_v\mathcal{O}_L = \prod \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}} I\mathcal{O}_L$$

where $I\mathcal{O}_L$ is coprime to the $\mathfrak{P}_i$. Now

$$\mathrm{ord}_{\mathfrak{P}}(\pi_v) = \mathrm{ord}_{\mathfrak{P}}(\prod \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}} I\mathcal{O}_L) = e_{\mathfrak{P}|\mathfrak{p}} = e$$

and

$$|\pi_v|_w = N(\mathfrak{P})^{-\mathrm{ord}_{\mathfrak{P}}(\pi_v)} = (N(\mathfrak{P})^{-1})^e = |\pi_w|_w^e.$$

□

This lemma also means that the ramification index coincides in the field extension and in its completion (this completes the same observation we have just made above for the inertial degree).

Example 7.6. Let

$$\begin{aligned} K_v &= \mathbb{Q}_p \\ L_w &= \mathbb{Q}_p(\sqrt[n]{p}) = \mathbb{Q}_p[X]/(X^n - p) \end{aligned}$$

The uniformizers are given by

$$\pi_v = p,\ \pi_w = \sqrt[n]{p}.$$

Thus

$$\begin{aligned} |\pi_w|_w &= 1/p \\ |\pi_v|_w &= 1/p^n \end{aligned}$$

which can be seen by noting that

$$|\pi_v|_w = |p|_w = |\sqrt[n]{p}|_w^n$$

which is the result of the Lemma. Thus

$$e = n$$

and the extension is totally ramified.

Example 7.7. Consider

$$\begin{aligned} K_v &= \mathbb{Q}_p \\ L_w &= \mathbb{Q}_p(\sqrt{\alpha}) = \mathbb{Q}_p[X]/(X^2 - \alpha) \end{aligned}$$

with $\alpha \in \mathbb{Z}_p^\times$, $\alpha \notin (\mathbb{Q}_p^\times)^2$. We have that π_w is still a uniformizer for L_w, but that $[\mathbb{F}_w : \mathbb{F}_v] = 2$.

The next theorem is a local version of the fact that if K is a number field, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Theorem 7.6. *The $\mathcal{O}_v$-module $\mathcal{O}_w$ is free of rank*

$$n_{w|v} = [L_w : K_v] = f_{w|v} e_{w|v}.$$

We give no proof, but just mention that the main point of the proof is the following: if $\{\beta_1, \ldots, \beta_f\} \subset \mathcal{O}_v$ is a set such that the reductions $\tilde{\beta}_i$ generates $\mathbb{F}_w$ as an $\mathbb{F}_v$-vector space, then the set

$$\{\beta_j \pi_w^k\}_{0 \le k \le e, 1 \le j \le f}$$

is an $\mathcal{O}_v$-basis of $\mathcal{O}_w$.

7.4 Normal extensions

Let L/K be a Galois extension of number fields. Recall that the decomposition group D of a prime $\mathfrak{P} \subset L$ is given by

$$D = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and that the inertia group I is the kernel of the map that sends an element of the Galois group in D to the Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. The corresponding fixed subfields help us to understand the ramification in L/K:

$$\begin{array}{c} L \\ \Big| e \\ L^I \\ \Big| f \\ L^D \\ \Big| g \\ K \end{array}$$

We further have that

$$[L : K] = efg$$

(note the contrast with the local case, where we have that

$$[L_w : K_v] = ef$$

by Theorem 7.6).

To analyze local extensions, that is, the extensions of completions, we can distinguish three cases:

Case 1. if $\mathfrak{p}$ completely splits in L, that is $g = [L : K]$ and $e = f = 1$, then

$$[L_w : K_v] = ef = 1$$

and $L_w = K_v$. This is the case described in Example 7.3, namely

$$K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{7}),\ K_v = \mathbb{Q}_3,\ L_w = \mathbb{Q}_3.$$

Case 2. if $\mathfrak{p}$ is inert, that is $g = e = 1$ and $f = [L : K]$, then

$$[L_w : K_v] = [L : K].$$

In this case, π_v is still a uniformizer for L_w, but $\mathbb{F}_w \neq \mathbb{F}_v$. This is a non-ramified extension. For example, consider

$$K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{7}),\ K_v = \mathbb{Q}_5,\ L_w = \mathbb{Q}_5(\sqrt{7}).$$

Case 3. If $\mathfrak{p}$ is totally ramified, that is $e = [L : K]$, then

$$[L_w : K_v] = [L : K]$$

but this time π_v is not a uniformizer for L_w, and $\mathbb{F}_w = \mathbb{F}_v$. For example, consider

$$K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{7}),\ K_v = \mathbb{Q}_7,\ L_w = \mathbb{Q}_7(\sqrt{7}).$$

Example 7.8. When does the Golden ratio $(1+\sqrt{5})/2$ belongs to $\mathbb{Q}_p$? It is easy to see that this question can be reformulated as: when is $\mathbb{Q}_p(\sqrt{5})$ an extension of $\mathbb{Q}_p$? Let us consider

$$K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{5}),\ K_v = \mathbb{Q}_p,\ L_w = \mathbb{Q}_p(\sqrt{5}).$$

Using the above three cases, we see that if p is inert or ramified in $\mathbb{Q}(\sqrt{5})$, then

$$[L_w : K_v] = [L : K] = 2$$

and the Golden ratio cannot be in $\mathbb{Q}_p$. This is the case for example for $p = 2, 3$ (inert), or $p = 5$ (ramified). On the contrary, if p splits, then $\mathbb{Q}_p = \mathbb{Q}_p(\sqrt{5})$. This is for example the case for $p = 11$ ($11 = (4 + \sqrt{5})(4 - \sqrt{5})$).

To conclude this section, let us note the following:

Proposition 7.7. *If L/K is Galois, we have the following isomorphism:*

$$D_{w|v} \simeq \mathrm{Gal}(L_w/K_v).$$

Compare this "local" result with the its "global" counterpart, where we have that D is a subgroup of $\mathrm{Gal}(L/K)$ of index $[\mathrm{Gal}(L/K) : D] = g$.

7.5 Finite extensions of $\mathbb{Q}_p$

Let $F/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. Then one can prove that F is the completion of a number field. In this section, we forget about this fact, and start by proving that

Theorem 7.8. *Let $F/\mathbb{Q}_p$ be a finite extension. Then there exists an absolute value on F which extends $|\cdot|_p$.*

Proof. Let $\mathcal{O}$ be the set of $\alpha \in F$ whose minimal polynomial over $\mathbb{Q}_p$ has coefficients in $\mathbb{Z}_p$. The set $\mathcal{O}$ is actually a ring (the proof is the same as in Chapter 1 to prove that $\mathcal{O}_K$ is a ring).

We claim that

$$\mathcal{O} = \{\alpha \in F \mid \mathrm{N}_{F/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p\}.$$

To prove this claim, we show that both inclusions hold. First, let us take $\alpha \in \mathcal{O}$, and prove that its norm is in $\mathbb{Z}_p$. If $\alpha \in \mathcal{O}$, then the constant coefficient a_0 of its minimal polynomial over $\mathbb{Q}_p$ is in $\mathbb{Z}_p$ by definition of $\mathcal{O}$, and

$$\mathrm{N}_{F/\mathbb{Q}_p}(\alpha) = \pm a_0^m \in \mathbb{Z}_p$$

for some positive m. For the reverse inclusion, we start with $\alpha \in F$ with $\mathrm{N}_{F/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$. Let

$$f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$$

be its minimal polynomial over $\mathbb{Q}_p$, with a priori $a_i \in \mathbb{Q}_p$, $i = 1, \ldots, m-1$. Since $\mathrm{N}_{F/\mathbb{Q}_p}(\alpha) \in \mathbb{Z}_p$, we have that $|a_0^m|_p \leq 1$, which implies that $|a_0|_p \leq 1$, that is $a_0 \in \mathbb{Z}_p$. We now would like to show that all $a_i \in \mathbb{Z}_p$, which is the same thing as proving that if p^k is the smallest power of p such that $g(X) = p^k f(X) \in \mathbb{Z}_p[X]$, then $k = 0$. Now let r be the smallest index such that $p^k a_r \in \mathbb{Z}_p^\times$ ($r \geq 0$ and $r > 0$ if $k > 0$ since then $p^k a_0$ cannot be a unit). We have (by choice of r) that

$$\begin{aligned} g(X) &\equiv p^k X^m + \ldots + p^k a_r X^r \mod p \\ &\equiv X^r(p^k X^{m-r} + \ldots + p^k a_r) \mod p. \end{aligned}$$

Hensel's lemma tells that g should have a factorization, which is in contradiction which the fact that $g(X) = p^k f(X)$ with $f(X)$ irreducible. Thus $r = 0$ and $p^k a_0 \in \mathbb{Z}_p^\times$ proving that $k = 0$.

Let us now go back to the proof of the theorem. We now set for all $\alpha \in F$:

$$|\alpha|_F = |\mathrm{N}_{F/\mathbb{Q}_p}(\alpha)|_p^{1/n}$$

where $n = [F : \mathbb{Q}_p]$. We need to prove that this is an absolute value, which extends $|\cdot|_p$.

- To show that it extends $|\cdot|_p$, let us restrict to $\alpha \in \mathbb{Q}_p$. Then

$$|\alpha|_F = |\mathrm{N}_{F/\mathbb{Q}_p}(\alpha)|_p^{1/n} = |\alpha^n|_p^{1/n} = |\alpha|_p.$$

- The two first axioms of the absolute value are easy to check:

$$|\alpha|_F = 0 \iff \alpha = 0,\ |\alpha\beta|_F = |\alpha|_F|\beta|_F.$$

- To show that $|\alpha + \beta|_F \leq \max\{|\alpha|_F, |\beta|_F\}$, it is enough to show, up to division by α or β, that

$$|\gamma|_F \leq 1 \Rightarrow |\gamma + 1|_F \leq 1.$$

  Indeed, if say $|\alpha/\beta|_F \leq 1$, then

$$|\alpha/\beta + 1|_F \leq 1 \leq \max\{|\alpha/\beta|_F, 1\}$$

  and vice versa. Now we have that

$$\begin{aligned} |\gamma|_F \leq 1 &\Rightarrow |\mathrm{N}_{F/\mathbb{Q}_p}(\gamma)|_p^{1/n} \leq 1 \\ &\Rightarrow |\mathrm{N}_{F/\mathbb{Q}_p}(\gamma)|_p \leq 1 \\ &\Rightarrow \mathrm{N}_{F/\mathbb{Q}_p}(\gamma) \in \mathbb{Z}_p \\ &\Rightarrow \gamma \in \mathcal{O} \end{aligned}$$

  by the claim above. Now since $\mathcal{O}$ is a ring, we have that both 1 and γ are in $\mathcal{O}$, thus $\gamma + 1 \in \mathcal{O}$ which implies that $|\gamma + 1|_F \leq 1$ and we are done.

□

We set

$$\mathfrak{m} = \{\alpha \in F \mid |\alpha|_F < 1\}$$

the unique maximal ideal of $\mathcal{O}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{m}$ is its residue class field, which is a finite extension of $\mathbb{F}_p$. We set the inertial degree to be $f = [\mathbb{F} : \mathbb{F}_p]$, and e to be such that $p\mathcal{O} = \mathfrak{m}^e$, which coincide with the definitions of e and f that we have already introduced.

We now proceed with studying finite extensions of $\mathbb{Q}_p$ based on their ramification. We start with non-ramified extensions.

Definition 7.3. A finite extension $F/\mathbb{Q}_p$ is non-ramified if $f = [F : \mathbb{Q}_p]$, that is $e = 1$.

Finite non-ramified extensions of $\mathbb{Q}_p$ are easily classified.

Theorem 7.9. *For each f, there is exactly one unramified extension of degree f. It can be obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^f - 1)$th root of unity.*

Proof. **Existence.** Let $\mathbb{F}_{p^f} = \mathbb{F}_p(\bar{\alpha})$ be an extension of $\mathbb{F}_p$ of degree f, and let

$$\bar{g}(X) = X^f + \bar{a}_{f-1}X^{f-1} + \ldots + \bar{a}_1 X + \bar{a}_0$$

be the minimal polynomial of $\bar{\alpha}$ over $\mathbb{F}_p$. Let us now lift $\bar{g}(X)$ to $g(X) \in \mathbb{Z}_p[X]$, which yields an irreducible polynomial over $\mathbb{Q}_p$. If α is a root of $g(X)$, then clearly $\mathbb{Q}_p(\alpha)$ is an extension of degree f of $\mathbb{Q}_p$. To complete the proof, it is now enough to prove that $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is a non-ramified extension of $\mathbb{Q}_p$, for which we just need to prove that is residue class field, say $\mathbb{F}_\mathfrak{p}$, is of degree f over $\mathbb{F}_p$. Since the residue class field contains a root of $g \mod \mathfrak{p}$ (this is just $\alpha \mod \mathfrak{p}$), we have that

$$[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \geq f.$$

On the other hand, we have that

$$[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \leq [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$$

which concludes the proof of existence.

Unicity. We prove here that any extension $F/\mathbb{Q}_p$ which is unramified and of degree f is equal to the extension obtained by adjoining a primitive (p^f-1)th root of unity. We already know by Corollary 7.3 that F must contain all the (p^f-1)th roots of unity. We then need to show that the smallest field extension of $\mathbb{Q}_p$ which contains the $(p^f - 1)$th roots of unity is of degree f. Let β be a $(p^f - 1)$th root of unity. We have that

$$\mathbb{Q}_p \subset \mathbb{Q}_p(\beta) \subset F.$$

But now, the residue class field of $\mathbb{Q}_p(\beta)$ also contains all the $(p^f - 1)$th roots of unity, so it contains $\mathbb{F}_{p^f}$, which implies that

$$[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \leq f.$$

□

Let us now look at totally ramified extensions.

Definition 7.4. A finite extension F of $\mathbb{Q}_p$ is totally ramified if $\mathbb{F} = \mathbb{F}_p$ (that is $f = 1$ and $e = n$).

Totally ramified extensions will be characterized in terms of Eisenstein polynomials.

Definition 7.5. The monic polynomial

$$f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0 \in \mathbb{Z}_p[X]$$

is called an Eisenstein polynomial if the two following conditions hold:

1. $a_i \in p\mathbb{Z}_p$,
2. $a_0 \notin p^2\mathbb{Z}_p$.

An Eisenstein polynomial is irreducible.

The classification theorem for finite totally ramified extensions of $\mathbb{Q}_p$ can now be stated.

Theorem 7.10. *1. If f is an Eisenstein polynomial, then $\mathbb{Q}_p[X]/f(X)$ is totally ramified.*

2. Let $F/\mathbb{Q}_p$ be a totally ramified extension and let π_F be a uniformizer. Then the minimal polynomial of π_F is an Eisenstein polynomial.

Example 7.9. $X^m - p$ is an Eisenstein polynomial for all $m \geq 2$, then $\mathbb{Q}_p(\sqrt[m]{p})$ is totally ramified.

Proof. 1. Let $F = \mathbb{Q}_p[X]/f(X)$, where

$$f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0$$

and let e be the ramification index of F. Set $m = [F : \mathbb{Q}_p]$. We have to show that $e = m$.

Let π be a root of f, then

$$\pi^m + a_{m-1}\pi^{m-1} + \ldots + a_1\pi + a_0 = 0$$

and

$$\mathrm{ord}_{\mathfrak{m}}(\pi^m) = \mathrm{ord}_{\mathfrak{m}}(a_{m-1}\pi^{m-1} + \ldots + a_0).$$

Since f is an Eisenstein polynomial by assumption, we have that $a_i \in p\mathbb{Z}_p \subset p\mathcal{O} = \mathfrak{m}^e$, so that

$$\mathrm{ord}_{\mathfrak{m}}(a_{m-1}\pi^{m-1} + \ldots + a_0) \geq e$$

and $\mathrm{ord}_{\mathfrak{m}}(\pi^m) \geq e$. In particular, $\mathrm{ord}_{\mathfrak{m}}(\pi) \geq 1$. Let s be the smallest integer such that

$$s \geq \frac{e}{\mathrm{ord}_{\mathfrak{m}}(\pi)}.$$

Then $m \geq e \geq s$. If $\mathrm{ord}_{\mathfrak{m}}(\pi^m) = e$, then $\mathrm{ord}_{\mathfrak{m}}(\pi) = \frac{e}{m}$ and thus $s = \frac{e}{e/m} = m$, and $m \geq e \geq m$ which shows that $m = e$. To conclude the proof, we need to show that $\mathrm{ord}_{\mathfrak{m}}(\pi^m) > e$ cannot possibly happen. Let us thus assume that $\mathrm{ord}_{\mathfrak{m}}(\pi^m) > e$. This implies that

$$\mathrm{ord}_{\mathfrak{m}}(a_0) = \mathrm{ord}_{\mathfrak{m}}(\pi^m + \pi(a_{m-1}\pi^{m-1} + \ldots + a_1)) > e.$$

Since $\mathrm{ord}_{\mathfrak{m}}(a_0) = \mathrm{ord}_p(a_0)e$, the second condition for Eisenstein polynomial shows that $\mathrm{ord}_{\mathfrak{m}}(a_0) = e$, which gives a contradiction.

2. We know from Theorem 7.6 that $\mathcal{O}$ is a free $\mathbb{Z}_p$-module, whose basis is given by

$$\{p^j \pi_F^k\}_{0 \leq k \leq e, 1 \leq j \leq f}$$

so that every element in F can be written as

$$\sum_{j,k} b_{jk} \pi_F^k p^j$$

and $F = \mathbb{Q}_p[\pi_F]$. Let

$$f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0$$

be the minimal polynomial of π_F. Then $\pm a_0 = N_{F/\mathbb{Q}_p}(\pi_F)$ is of valuation 1, since π_F is a uniformizer and $F/\mathbb{Q}_p$ is totally ramified. Let us look at $\tilde{f}$, the reduction of f in $\mathbb{F}_p[X]$. Since $\mathbb{F}_p[X]$ is a unique factorization domain, we can write

$$\tilde{f}(X) = \prod \phi_i^{k_i}$$

where ϕ_i are irreducible distinct polynomials in $\mathbb{F}_p[X]$. By Hensel's lemma, we can lift this factorization into a factorization $f = \prod f_i$ such that $\tilde{f}_i = \phi_i^{k_i}$. Since f is irreducible (it is a minimal polynomial), we have only one factor, that is $f = f_1$, and $\tilde{f}_1 = \phi_1^{k_1}$. In words, we have that $\tilde{f}$ is a power of an irreducible polynomial in $\mathbb{F}_p[X]$. Then $\tilde{f} = (X - a)^m$ since $\tilde{f}$ must have a root in $\mathbb{F}_p = \mathbb{F}$. Since $a_0 \equiv 0 \mod p$, we must have $a \equiv 0 \mod p$ and $\tilde{f} \equiv X^m \mod p$. In other words, $a_i \in p\mathbb{Z}_p$ for all i. This tells us that $f(X)$ is an Eisenstein polynomial.

□

The main definitions and results of this chapter are

- Definition of the completion K_ν of a number field K, of uniformizer.
- Hensel's Lemmas.
- Local ramification index $e_{w|v}$ and inertial degree $f_{w|v}$, and the local formula $n_{w|v} = e_{w|v} f_{w|v}$.
- Classification of extensions of $\mathbb{Q}_p$: either non-ramified (there a unique such extension) or totally ramified.