http://dx.doi.org/10.1090/surv/191/12

APPENDIX B

A glimpse of number theory

In this appendix, we recall without proof some well-known facts on local fields and number fields.

B.1. Absolute values

We define the notion of an absolute value. There are several slightly different definitions of this notion. We will take the point of view of [**31**], but some references cited here choose another one. However, the choice of the definition does not have any influence on the validity of the theorems listed in this appendix. Notice that what we call an absolute value here is called a valuation in [**31**].

DEFINITION B.1.1. Let K be a field. An **absolute value** on K is a map $\upsilon : K \longrightarrow \mathbb{R}^+$ such that:

(1) for all $x \in K$, $\upsilon(x) = 0 \iff x = 0$;

(2) for all $x, y \in K$, $\upsilon(xy) = \upsilon(x)\upsilon(y)$;

(3) for all $x, y \in K$, $\upsilon(x + y) \leq \upsilon(x) + \upsilon(y)$.

We will say that υ is **archimedean** if $\mathrm{char}(K) = 0$ and there exists $m \in \mathbb{Z}$ such that $\upsilon(m{\cdot}1_K) > 1$, and **non-archimedean** otherwise.

The **trivial** absolute value is the absolute value υ such that $\upsilon(0) = 0$ and $\upsilon(x) = 1$ for all $x \in K^\times$.

Two absolute values υ_1 and υ_2 are **equivalent** if there exists $\lambda \in \mathbb{R}^{+\times}$ such that $\upsilon_2 = \upsilon_1^\lambda$.

One may show that two absolute values are equivalent if and only if they define the same topology on K (cf. [**31**, Theorem 4.1.1]). A **place** of K is an equivalence class of absolute values.

REMARK B.1.2. If υ is an absolute value on K and $s > 0$, then υ^s is not necessarily an absolute value, as the example of the ordinary absolute value on $\mathbb{R}$ already shows. □

EXAMPLES B.1.3.

(1) Let υ_∞ be the ordinary absolute value on $\mathbb{Q}$. Then υ_∞ is an archimedean absolute value.

(2) Let p be a prime number. For all $x \in \mathbb{Q} \setminus \{0\}$, we denote by $n_p(x)$ the p-adic valuation of x. We also set $n_p(0) = -\infty$. Then the map

$$\upsilon_p : \begin{array}{c} \mathbb{Q} \longrightarrow \mathbb{R}^+ \\ x \longmapsto p^{-n_p(x)} \end{array}$$

is a non-archimedean absolute value on $\mathbb{Q}$.

□

REMARK B.1.4. A theorem of Ostrowski shows that υ_∞ and the absolute values υ_p, p prime, form a complete set of pairwise non-equivalent absolute values on $\mathbb{Q}$. We will generalize this statement later on. □

If υ is an absolute value on K, we can construct the completion $\hat{K}$ with respect to this absolute value, in the same way we construct $\mathbb{R}$ from $\mathbb{Q}$. This field contains K as a subfield (or more precisely a subfield canonically isomorphic to K) and is equipped with an absolute value which restricts to υ on K (see [**31**], Section 4.3). In view of this, this new absolute value will still be denoted by υ. Moreover, $\hat{K}$ is complete for the topology defined by υ. Two equivalent absolute values will give rise to the same field $\hat{K}$, and the extension of these absolute values to $\hat{K}$ will be equivalent.

EXAMPLE B.1.5. The completion of $\mathbb{Q}$ with respect to υ_∞ is the field of real numbers $\mathbb{R}$, while the completion of $\mathbb{Q}$ with respect to υ_p is the field of p-adic numbers $\mathbb{Q}_p$. □

DEFINITION B.1.6. Let υ be a non-archimedean absolute value on a field K. The set

$$\mathcal{O}_\upsilon = \{x \in K | \upsilon(x) \leq 1\}$$

is a commutative ring, called the **valuation ring** of (K, υ). It is a local ring, with unique maximal ideal

$$\mathfrak{m}_\upsilon = \{x \in K | \upsilon(x) < 1\}.$$

Therefore, the units of $\mathcal{O}_K$ are

$$\mathcal{O}_\upsilon^\times = \{x \in K | \upsilon(x) = 1\}.$$

The **residue field** of (K, υ) is the field $\kappa(\upsilon) = \mathcal{O}_\upsilon / \mathfrak{m}_\upsilon$. One can show that υ and its extension to K_υ have canonically isomorphic residue fields.

DEFINITION B.1.7. We say that υ is **discrete** if $\upsilon(K^\times)$ is a discrete subgroup of $\mathbb{R}^{+\times}$. Any discrete absolute value is non-archimedean.

EXAMPLE B.1.8. For every prime p, υ_p is a discrete absolute value on $\mathbb{Q}$. Indeed, $\upsilon_p(\mathbb{Q}^\times)$ is the cyclic group of $\mathbb{R}^{+\times}$ generated by p, which is discrete, since it isomorphic to $\mathbb{Z}$. □

Non-trivial discrete absolute values have some nice properties.

PROPOSITION B.1.9. *Let υ be a non-trivial discrete absolute value on a field K. Then $\mathcal{O}_\upsilon$ is a principal ideal domain, with field of fractions K, and $\mathfrak{m}_\upsilon$ is generated by an element $\pi_\upsilon \in \mathfrak{m}_\upsilon$.*

Moreover, any $x \in K^\times$ may be written in a unique way as

$$x = u\pi^{n_\upsilon(x)}, u \in \mathcal{O}_\upsilon^\times, n_\upsilon(x) \in \mathbb{Z}.$$

DEFINITION B.1.10. Let υ be a non-trivial discrete absolute value on a field K. Any generator $\pi_\upsilon \in \mathfrak{m}_\upsilon$ is called a **local parameter**.

EXAMPLE B.1.11. Let p be a prime number. Then p is a local parameter for the absolute value υ_p on $\mathbb{Q}$. □

REMARK B.1.12. If υ is a non-trivial discrete valuation on K, with local parameter π_υ, it follows from the last part of Proposition B.1.9 that we have

$$\upsilon(K^\times) = \langle \upsilon(\pi_\upsilon) \rangle.$$

□

DEFINITION B.1.13. Let L/K be a field extension, let υ and w be two non-trivial discrete absolute values on K and L respectively.

If $w_{|_K} = \upsilon$, we say that w **extends** υ, or that w is an extension of υ , and we denote it by $w|\upsilon$. In this case, we have

$$\mathfrak{m}_w = \mathfrak{m}_\upsilon \cap K.$$

In particular, $\kappa(w) \supset \kappa(\upsilon)$. The degree of $\kappa(w)/\kappa(\upsilon)$ is called **the residual degree of** w **over** υ and is denoted by $f_{w|\upsilon}$ (it may be infinite).

The index $[w(L^\times) : \upsilon(K^\times)]$ is finite and called **the ramification index of** w **over** υ; it is denoted by $e_{w|\upsilon}$.

We say that the extension $(L, w)/(K, \upsilon)$ is

(1) **unramified** if $e_{w|\upsilon} = 1$;
(2) **ramified** if $e_{w|\upsilon} > 1$;
(3) **totally ramified** if it is ramified and $\kappa(w) = \kappa(\upsilon)$.

REMARK B.1.14. Let $(L, w)/(K, \upsilon)$ be an extension of non-trivial discrete absolute values, and let π_υ and π_w be local parameters for υ and w respectively. By the last part of Proposition B.1.9, we may write

$$\pi_\upsilon = u\pi_w^e, u \in \mathcal{O}_w^\times, e \geq 1,$$

taking into account that we cannot have $e \leq 0$, since otherwise, we would have

$$\upsilon(\pi_\upsilon) = w(\pi_\upsilon) = w(\pi_w)^e > 1,$$

contradicting the fact that $\pi_\upsilon \in \mathfrak{m}_\upsilon$.

Set $a = w(\pi_w)$, so that $\upsilon(\pi_\upsilon) = a^e$. By Remark B.1.12, $w(L^\times)$ and $\upsilon(K^\times)$ are generated respectively by a and a^e. It follows that we have

$$e_{w|\upsilon} = [\langle a \rangle : \langle a^e \rangle] = e.$$

In other words, the ramification index of $(L, w)/(K, \upsilon)$ is also the unique integer $e_{w|\upsilon}$ such that

$$\pi_\upsilon = u\pi_w^{e_{w|\upsilon}}, u \in \mathcal{O}_w^\times,$$

where π_υ and π_w are local parameters of υ and w respectively.

In particular, $(L, w)/(K, \upsilon)$ is unramified if and only if π_υ is a local parameter for w. □

EXAMPLE B.1.15. Recall that $\mathbb{Z}[i]$ is a principal ideal domain, with field of fractions $\mathbb{Q}(i)$. For any irreducible element π of $\mathbb{Z}[i]$, we may consider the π-adic valuation $n_\pi(x)$ of an element x (as usual, we set $n_\pi(0) = -\infty$).

(1) Recall that $1+i$ is a prime element of $\mathbb{Z}[i]$. Since $2 = -i(1+i)^2$, it follows that the map

$$w\colon \begin{array}{ccc} \mathbb{Q}(i) & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & \sqrt{2}^{-n_{1+i}(x)} \end{array}$$

is a non-trivial discrete absolute value, with local parameter $1+i$, which extends the absolute value v_2 on $\mathbb{Q}$. Moreover, the corresponding ramification index is 2.

(2) The element $1+2i$ is a prime element of $\mathbb{Z}[i]$. Since we have the equality $5 = (1-2i)(1+2i)$ and $1+2i$ is not associate to $1-2i$, it follows that the map

$$w\colon \begin{array}{ccc} \mathbb{Q}(i) & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & 5^{-n_{1+2i}(x)} \end{array}$$

is a non-trivial discrete absolute value, with local parameter $1-2i$, which extends the absolute value v_5 on $\mathbb{Q}$. Moreover, the corresponding ramification index is 1.

We will see a generalization of these examples in a forthcoming section. □

We now define local fields.

DEFINITION B.1.16. A **local field** is a field K of characteristic zero which is complete for a non-trivial discrete absolute value v, such that $\kappa(v)$ is finite.

THEOREM B.1.17. *Let L/K be a field extension of degree n, where (K, v) is a local field. Then v extends in a unique way to a non-trivial discrete absolute value w, for which L is complete. Hence, L is also a local field. Moreover, we have*

$$n = e_{w|v} f_{w|v}.$$

In particular, L/K is **totally ramified** *if and only if $e_{w|v} = n$.*

REMARK B.1.18. This theorem shows in particular that any finite extension of $\mathbb{Q}_p$ is a local field. One may prove that the converse holds as well (see [**31**, Theorem 4.7.1], noticing that we have assumed in this appendix that a local field has characteristic zero). The reader will find a proof of this theorem in [**31**], Section 4.5. □

We end this section by describing the unramified extensions and the totally ramified extensions of a local field.

PROPOSITION B.1.19. *Let (K, v) be a local field and let $\kappa(v) \simeq \mathbb{F}_q$, where $q = p^f$, for some prime p.*

Then for any integer $m \geq 1$ prime to p, the extension $K(\zeta_m)/K$ is unramified and cyclic of degree d, where d is the order of $\overline{q}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Moreover, there exists a canonical generator φ_m for $\mathrm{Gal}(K(\zeta_m)/K)$, uniquely determined by the condition

$$\varphi_m(x) \equiv x^q \mod \pi_L, \text{ for all } x \in \mathcal{O}_L.$$

Conversely, for a given $n \geq 1$, there is a unique unramified extension L/K of degree n, up to K-isomorphism. This extension is cyclic and isomorphic to $K(\zeta_{q^n-1})/K$.

See [**44**, Chapter IV, §4, Proposition 16] for a proof.

DEFINITION B.1.20. The canonical generator of the unique unramified extension L/K of degree n is called the **Frobenius map**, and is denoted by $\mathrm{Frob}(L/K)$.

PROPOSITION B.1.21. *Let (K, v) be a local field.*

A field extension L/K of degree n is totally ramified if and only if L is generated by an element $\alpha \in L$ such that

$$\mu_{\alpha,K} = X^b + a_{n-1}X^{n-1} + \cdots + a_0, n_v(a_i) \geq 1, n_v(a_0) = 1.$$

Moreover, if $\mathrm{char}(v) \nmid n$, and L/K is a Galois totally ramified extension of degree n, then $\mu_n \subset K$ and there exists and local parameter π_v such that $L = K(\sqrt[n]{\pi_K})$.

See [**11**],Theorem 1, p.23 and Proposition 1, p.32 for a proof.

B.2. Factorization of ideals in number fields

DEFINITION B.2.1. A **number field** is a field extension $K/\mathbb{Q}$ of finite degree. The **ring of integers** of K, denoted by $\mathcal{O}_K$, is the subset of elements $x \in K$ which are roots of monic polynomials of $\mathbb{Z}[X]$. It is a subring of K, and its field of fractions is isomorphic to K (apply the results of [**43**] , Section 5.1 to $A = \mathbb{Z}$ and $R = K$).

Moreover, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$ ([**43**, 6.3, Theorem 2]).

EXAMPLES B.2.2.

(1) Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is a non-zero square-free integer. Then we have:
   (*i*) $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1[4]$;
   (*ii*) $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1[4]$.
(2) Let $K = \mathbb{Q}(\zeta_n), n \geq 1$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

See [**43**], Sections 5.1 and 16.2 for more details. □

The following theorem is the starting point of algebraic number theory.

THEOREM B.2.3. *Let K be a number field. Then the following properties hold:*

(1) *for every non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$, we have $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{a} \supset \mathfrak{b}$;*
(2) *every non-zero prime ideal $\mathfrak{p}$ is maximal and $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is a finite field;*
(3) *every non-zero ideal of $\mathcal{O}_K$ decomposes in a unique way (up to permutation) as a product of prime ideals.*

See [**43**], Section 7.1, Part A. and Theorem 1, and Section 7.2.F, for example.

For any non-zero ideal $\mathfrak{a}$, we may then consider its $\mathfrak{p}$-adic valuation $n_\mathfrak{p}(\mathfrak{a})$ for any prime ideal $\mathfrak{p}$. We also set $n_\mathfrak{p}(0) = -\infty$.

Let $x \in K$, and write $x = \dfrac{a}{b}, a, b \in \mathcal{O}_k$. Then we set

$$n_\mathfrak{p}(x) = n_\mathfrak{p}(a\mathcal{O}_K) - n_\mathfrak{p}(b\mathcal{O}_K).$$

One may check easily that it does not depend on the choice of a and b.

EXAMPLE B.2.4. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $n \geq 1$. Then for any element $a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$, we have

$$n_{\mathfrak{p}}(a) = n.$$

Indeed, by assumption, we have $(a) \subset \mathfrak{p}^n$ and $(a) \not\subset \mathfrak{p}^{n+1}$. The first point of Theorem B.2.3 then shows that $\mathfrak{p}^n \mid (a)$ but $\mathfrak{p}^{n+1} \nmid (a)$, that is $n_{\mathfrak{p}}(a) = n$. □

If $\mathcal{O}_K$ is a principal ideal domain, every prime ideal $\mathfrak{p}$ is principal, generated by a prime element $\pi \in \mathcal{O}_K$. In this case, we will write n_π rather than $n_{(\pi)}$. If $x \in K$, the integer $n_\pi(x)$ does not depend on the choice of π.

We continue with the following approximation lemma.

LEMMA B.2.5. *Let K be a number field. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be r distinct prime ideals of $\mathcal{O}_K$, and let $n_1, \ldots, n_r \in \mathbb{Z}$. Then there exists $x \in K$ satisfying the following conditions:*

(1) $n_{\mathfrak{p}_i}(x) = n_i$ *for* $i = 1, \ldots, r$;
(2) $n_{\mathfrak{p}}(x) \geq 0$ *for any prime ideal* $\mathfrak{p} \neq \mathfrak{p}_i, i = 1, \ldots, r$.

Proof. Assume first that $n_1, \ldots, n_r$ are non-negative integers. Since the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are all distinct, the ideals $\mathfrak{p}_1^{n_1}, \ldots, \mathfrak{p}_r^{n_r}$ are pairwise coprime. For each i, pick $a_i \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$ (such an element a_i exists since $\mathfrak{p}_i^{n_i} \neq \mathfrak{p}_i^{n_i+1}$ by the uniqueness of the decomposition into a product of prime ideals).

By the Chinese Remainder Theorem, there exists $a \in \mathcal{O}_K$ such that $a \equiv a_i \mod \mathfrak{p}_i^{n_i}$ for $i = 1, \ldots, r$. Since $a_i \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$ and $\mathfrak{p}_i^{n_i+1} \subset \mathfrak{p}_i^{n_i}$, we also have $a \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$. By Example B.2.4, we get $n_{\mathfrak{p}_i}(a) = n_i$ for $i = 1, \ldots, r$. The second condition is automatically satisfied since $a \in \mathcal{O}_K$.

Let us go back to the general case. Renumbering if necessary, we may assume that $n_1, \ldots, n_s \geq 0$ and $n_{s+1}, \ldots, n_r \leq 0$. By the previous point, there exists $b \in \mathcal{O}_K$ such that:

(i) $n_{\mathfrak{p}_i}(b) = 0$ for $i = 1, \ldots, s$;

(ii) $n_{\mathfrak{p}_i}(b) = -n_i$ for $i = s+1, \ldots, r$.

In particular, we may write

$$(b) = \mathfrak{p}_1^{-n_{s+1}} \cdots \mathfrak{p}_r^{-n_r} \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_t^{m_t},$$

where $\mathfrak{q}_j \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ for all j, and $m_j > 0$. One may then find $a \in \mathcal{O}_K$ satisfying the following conditions:

(iii) $n_{\mathfrak{p}_i}(a) = n_i$ for $i = 1, \ldots, s$;

(iv) $n_{\mathfrak{p}_i}(a) = 0$ for $i = s+1, \ldots, r$;

(v) $n_{\mathbb{Q}_j}(a) = m_j$ for $j = 1, \ldots, t$.

Set $x = \dfrac{a}{b}$. We claim that x satisfies the required conditions. Indeed, for $i = 1, \ldots, s$, we have

$$n_{\mathfrak{p}_i}(x) = n_{\mathfrak{p}_i}(a) - n_{\mathfrak{p}_i}(b) = n_i - 0 = n_i$$

by (i) and (ii), and for $i = s+1, \ldots, r$, we have

$$n_{\mathfrak{p}_i}(x) = 0 - (-n_i) = n_i$$

by (ii) and (iv).

Assume now that $\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. If $\mathfrak{p} \neq \mathfrak{q}_1, \ldots, \mathfrak{q}_t$, we have

$$n_{\mathfrak{p}}(x) = n_{\mathfrak{p}}(a) - n_{\mathfrak{p}}(b) = n_{\mathfrak{p}}(a) \geq 0,$$

since $n_{\mathfrak{p}}(b) = 0$ in view of the decomposition of (b) above. Finally, for $j = 1, \ldots, t$, we have

$$n_{\mathfrak{q}_j}(x) = n_{\mathfrak{q}_j}(a) - n_{\mathfrak{q}_j}(b) = m_j - m_j = 0.$$

This concludes the proof. □

DEFINITION B.2.6. Let L/K be a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. We say that a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ **lies above** $\mathfrak{p}$ if we have

$$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}.$$

We denote it by $\mathfrak{P} \mid \mathfrak{p}$.

In this case, $\kappa(\mathfrak{p})$ identifies canonically to a subfield of $\kappa(\mathfrak{P})$, so that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is an extension of finite fields.

EXAMPLE B.2.7. Let $K = \mathbb{Q}$ and let $K = \mathbb{Q}(i)$. Then $(1+i)\mathbb{Z}[i]$ is a prime ideal of $\mathcal{O}_L = \mathbb{Z}[i]$ lying above $2\mathbb{Z}$. □

PROPOSITION B.2.8. *Let L/K be a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lies above $\mathfrak{p}$ if and only if $n_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L) \geq 1$, that is $\mathfrak{P}$ appears in the decomposition of $\mathfrak{p}\mathcal{O}_L$ into a product of prime ideals of $\mathfrak{p}\mathcal{O}_L$.*

DEFINITION B.2.9. Let L/K be a finite extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, e_r \geq 1,$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are pairwise distinct prime ideals of $\mathcal{O}_L$.

If $\mathfrak{P} \mid \mathfrak{p}$, then $\mathfrak{P} = \mathfrak{P}_i$ for some i, and the integer e_i is called the **ramification index** of $\mathfrak{P}$ over $\mathfrak{p}$; it is denoted by $e_{\mathfrak{P}|\mathfrak{p}}$. In other words, for all $\mathfrak{P} \mid \mathfrak{p}$, we have

$$e_{\mathfrak{P}|\mathfrak{p}} = n_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L).$$

The degree $f_{\mathfrak{P}|\mathfrak{p}} = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$ is called the **residual degree** of $\mathfrak{P}$ over $\mathfrak{p}$.

We say that:

(1) $\mathfrak{p}$ **does not ramify** in L, or is **unramified** if $e_{\mathfrak{P}|\mathfrak{p}} = 1$ for all $\mathfrak{P} \mid \mathfrak{p}$;
(2) $\mathfrak{p}$ **is inert** in L if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$;
(3) $\mathfrak{p}$ **totally splits** in L if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, where $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$ are $n = [L : K]$ distinct prime ideals of $\mathcal{O}_L$;
(4) $\mathfrak{p}$ **ramifies** in L if $e_{\mathfrak{P}|\mathfrak{p}} > 1$ for some $\mathfrak{P} \mid \mathfrak{p}$;
(5) $\mathfrak{p}$ **totally ramifies** in L if $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$, for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, where $n = [L : K]$;
(6) $\mathfrak{p}$ **tamely ramifies** in L if $\mathfrak{p}$ ramifies and $e_{\mathfrak{P}|\mathfrak{p}}$ is prime to $\mathrm{char}(\kappa(\mathfrak{p}))$ for all $\mathfrak{P} \mid \mathfrak{p}$, and **wildly ramifies otherwise.**

If $\mathcal{O}_K$ is a principal ideal domain, the prime ideals are generated by the irreducible elements of $\mathcal{O}_K$. In this case, we will say that an irreducible element π of $\mathcal{O}_K$ ramifies (resp. is inert etc.) instead of (π) ramifies (resp. is inert, etc.).

PROPOSITION B.2.10. *Let L/K be an extension of number fields, and let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$. Then we have*

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}.$$

See for example [**31**, (3.10.2)].

The next proposition shows that factorisation of prime ideals is particularly nice in Galois extensions (see [**31**], Proposition 6.1.1 and equality (3.10.2)).

PROPOSITION B.2.11. *Let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then G acts transitively of the set of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$. In particular, the integers $e_\mathfrak{p} = e_{\mathfrak{P}|\mathfrak{p}}$ and $f_\mathfrak{p} = f_{\mathfrak{P}|\mathfrak{p}}$ do not depend on the choice of a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$.*

Moreover, if $g_\mathfrak{p}$ denotes the number of prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$, we have

$$[L : K] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}.$$

The following theorem is very useful to decompose prime ideals of a number field K, especially when $\mathcal{O}_K = \mathbb{Z}[\theta]$ (see [**31**, Theorem 3.8.2] for a proof).

THEOREM B.2.12 (Dedekind). *Let K be a number field, and let $\theta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$. For all $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, let $\overline{\mu_{\theta,\mathbb{Q}}} \in \mathbb{F}_p[X]$ be the reduction of the minimal polynomial of θ modulo p, and write*

$$\overline{\mu_{\theta,\mathbb{Q}}} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r},$$

where $g_1, \ldots, g_r \in \mathbb{Z}[X]$ are pairwise distinct monic polynomials which are irreducible modulo p and $e_i \geq 1$.

For $i = 1, \ldots, r$, set $\mathfrak{p}_i = (p, g_i(\theta))$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are pairwise distinct prime ideals of $\mathcal{O}_K$ and we have

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

REMARK B.2.13. If $\mathcal{O}_k = \mathbb{Z}[\theta]$, then the condition $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ is always fulfilled, and one may obtain the decomposition of $p\mathcal{O}_K$ for any prime p. □

As an example, we describe the ramification of prime numbers in a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.

EXAMPLE B.2.14. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ be a non-zero square free integer, and let p be a prime number.

Assume first that $d \not\equiv 1[4]$. In this case, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Since $X^2 - d$ is the minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$, we get the following results.

(1) If $p = 2$ or $p \mid d$, then $X^2 - d$ is a square modulo $\mathbb{F}_p$, since it is equal to X^2 or $(X-1)^2$ in all cases. Hence p totally ramifies.

(2) If p is odd, $p \nmid d$ and $d \notin \mathbb{F}_p^{\times 2}$, then $X^2 - d \in \mathbb{F}_p[X]$ is irreducible, and p is inert in $K/\mathbb{Q}$.

(3) If p is odd, $p \nmid d$ and $d \in \mathbb{F}_p^{\times 2}$, then $X^2 - d \in \mathbb{F}_[X]$ is the product of two distinct polynomials of degree 1, and p totally splits in $K/\mathbb{Q}$.

Assume now that $d \equiv 1[4]$, so that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Since $X^2 - X + \frac{1-d}{4}$ is the minimal polynomial of $\dfrac{1+\sqrt{d}}{2}$ over $\mathbb{Q}$, we get the following results.

(4) Assume that $p = 2$. If $d \equiv 5[8]$, then $X^2 - X + \frac{1-d}{4}$ is irreducible modulo 2 since it is equal to $X^2 - X - 1 \in \mathbb{F}_2[X]$ in this case, and 2 is inert. If $d \equiv 1[8]$, then $X^2 - X + \frac{1-d}{4}$ is equal to $X(X-1) \in \mathbb{F}_2[X]$ in this case, and 2 totally splits.

(5) If $p \mid d$ (so p is odd), then $X^2 - X + \frac{1-d}{4}$ is a square modulo $\mathbb{F}_p$, since it is equal to $(X - 1/2)^2$. Hence p totally ramifies.

(6) If p is odd, $p \nmid d$ and $d \notin \mathbb{F}_p^{\times 2}$, then $X^2 - X + \frac{1-d}{4} \in \mathbb{F}_p[X]$ is irreducible, and p is inert in $K/\mathbb{Q}$.

(7) If p is odd, $p \nmid d$ and $d \in \mathbb{F}_p^{\times 2}$, then $X^2 - X + \frac{1-d}{4} \in \mathbb{F}_p[X]$ is the product of two distinct polynomials of degree 1, and p totally splits in $K/\mathbb{Q}$.

□

The case of cyclotomic extensions is also well-known (see [**31**], Propositions 6.4.6 and 6.4.8 for example).

THEOREM B.2.15. *Let $m \geq 3$ be an integer. Assume that $4 \mid m$ if m is even, and let $L = \mathbb{Q}(\zeta_m)$. For any p prime number, the ramification index e_p is equal to $\varphi(p^{n_p(m)})$, and the residual degree f_p is the multiplicative order of p modulo $\dfrac{m}{p^{n_p(m)}}$.*

COROLLARY B.2.16. *Let $m \geq 3$ be an integer. Assume that $4 \mid m$ if m is even, and let p be a prime number. Then the following properties hold:*

(1) *p ramifies in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if $p \mid m$;*

(2) *p is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if $p \nmid m$;*

(3) *p totally splits in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if $p \equiv 1[m]$;*

(4) *p is inert in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if $\overline{p}$ is a generator of $(\mathbb{Z}/m\mathbb{Z})^\times$.*

We are now interested in the existence of prime ideals having a prescribed behavior in a Galois extension. We start with the case of unramified primes. In this case, the results of Section 25.1.A of [**43**] and Tchebotarev's Density Theorem (see [**43**], Section 25.3, Theorem 1) imply the following result.

PROPOSITION B.2.17. *Let L/K be a Galois extension of number fields. Then the following properties hold:*

(1) *there are infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which totally splits in L;*

(2) *there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ which stays inert in L if and only if L/K is cyclic. In this case, the number of such prime ideals is infinite.*

We will also need the following result (see [**31**], Propositions 4.9.1 and 4.9.2 for a proof).

LEMMA B.2.18. *Let L_1/K and L_2/K be two extensions of a number field K, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. If $\mathfrak{p}$ is unramified (resp. splits completely) in L_1 and L_2, then $\mathfrak{p}$ is unramified (resp. splits completely) in L_1L_2.*

We are now interested in the existence of ramified ideals. First, we need to define the norm of an ideal. The Chinese Remainder Theorem and Theorem B.2.3 show that for any non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the quotient ring $\mathcal{O}/\mathfrak{a}$ is finite. Therefore, the following definition makes sense.

DEFINITION B.2.19. Let K be a number field. For any non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we set

$$N_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

The integer $N_{K/\mathbb{Q}}(\mathfrak{a})$ is called the **absolute norm** of $\mathfrak{a}$.

PROPOSITION B.2.20. *Let K be a number field, and let $\mathfrak{a}, \mathfrak{b}$ be two ideals of $\mathcal{O}_K$. Then the following properties hold:*

(1) *we have $N_{K/\mathbb{Q}}(\mathfrak{ab}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{b})$;*
(2) *if $\mathfrak{a} \supset \mathfrak{b}$, then $N_{K/\mathbb{Q}}(\mathfrak{a}) \mid N_{K/\mathbb{Q}}(\mathfrak{b})$. Moreover, equality holds if and only if $\mathfrak{a} = \mathfrak{b}$;*
(3) *for all $x \in K^\times$, we have $N_{K/\mathbb{Q}}(x\mathcal{O}_K) = |N_{K/\mathbb{Q}}(x)|$.*

We will also need a relative version of the norm.

DEFINITION B.2.21. Let L/K be an extension of number fields. For any ideal $\mathfrak{A}$ of $\mathcal{O}_L$, we denote by $\mathcal{N}_{L/K}(\mathfrak{A})$ the ideal of $\mathcal{O}_K$ generated by the elements $N_{L/K}(x), x \in \mathfrak{A}$, and call it the **relative norm** of $\mathfrak{A}$.

We then have the following properties.

PROPOSITION B.2.22. *Let L/K be an extension of number fields, and let $\mathfrak{A}, \mathfrak{B}$ be two ideals of $\mathcal{O}_L$. Then the following properties hold:*

(1) *if $K = \mathbb{Q}$, we have $\mathcal{N}_{L/\mathbb{Q}}(\mathfrak{A}) = N_{L/\mathbb{Q}}(\mathfrak{A})\mathbb{Z}$;*
(2) *we have $\mathcal{N}_{L/K}(\mathfrak{AB}) = \mathcal{N}_{L/K}(\mathfrak{A})\mathcal{N}_{L/K}(\mathfrak{B})$;*
(3) *if $\mathfrak{A} \supset \mathfrak{B}$, then $\mathcal{N}_{L/K}(\mathfrak{A}) \subset \mathcal{N}_{L/K}(\mathfrak{B})$. Moreover, equality holds if and only if $\mathfrak{A} = \mathfrak{B}$;*
(4) *if $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, then $\mathcal{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}}$;*
(5) *if L/K is a Galois extension with Galois group G, then we have*

$$\mathcal{N}_{L/K}(\mathfrak{A}) = \big(\prod_{\sigma \in G} \sigma(\mathfrak{A})\big) \cap \mathcal{O}_K;$$

(6) *if $K \subset M \subset L$, we have*

$$\mathcal{N}_{L/K}(\mathfrak{A}) = \mathcal{N}_{M/K}(\mathcal{N}_{L/M}(\mathfrak{A})).$$

In particular, if $K = \mathbb{Q}$, we have

$$N_{L/\mathbb{Q}}(\mathfrak{A}) = N_{M/\mathbb{Q}}(\mathcal{N}_{L/M}(\mathfrak{A}));$$

(7) *if $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then $\mathcal{N}_{L/K}(\mathfrak{a}) = \mathfrak{a}^{[L:K]}$.*

See [**26**] , [**28**], [**31**] or [**43**, Section 13.1].

REMARK B.2.23. Properties (3) and (4) show in particular that, for any non-zero ideal $\mathfrak{A}$ of $\mathcal{O}_L$, a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ dividing $\mathfrak{A}$ necessary lie above a prime ideal $\mathfrak{p}$ dividing $\mathcal{N}_{L/k}(\mathfrak{A})$. □

We would like now to give a characterization of the prime ideals $\mathfrak{p}$ which ramify in L. First, we need some definitions.

DEFINITION B.2.24. Let L/K be an extension of number fields. Let $\mathbf{w} = (w_1, \cdots, w_n)$ be a K-basis of L contained in $\mathcal{O}_L$ (i.e. $w_i \in \mathcal{O}_L$ for all i). The **discriminant** $D(\mathbf{w})$ of $\mathbf{w}$ is the determinant of the matrix $(\mathrm{Tr}_{L/K}(w_i w_j))$. This is an element of $\mathcal{O}_K$.

The **discriminant ideal** $\mathcal{D}_{L/K}$ is the ideal of $\mathcal{O}_K$ generated by the elements $D(\mathbf{w})$, for all K-bases $\mathbf{w}$ of L contained in $\mathcal{O}_L$.

If $\mathcal{O}_K$ is a principal ideal domain, it is the ideal generated by the discriminant of an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. In particular, if $K = \mathbb{Q}$, the absolute value of the discriminant of a $\mathbb{Z}$-basis of $\mathcal{O}_L$, and does not depend on the choice of this basis. It is denoted by $\mathrm{disc}(L)$, and called the **absolute discriminant** of K. In other words, $\mathrm{disc}(L)$ is the unique positive integer such that

$$\mathcal{D}_{L/\mathbb{Q}} = \mathrm{disc}(L)\mathbb{Z}.$$

The **different ideal** of L/K is the ideal $\mathfrak{d}_{L/K}$ of $\mathcal{O}_L$ generated by the elements $f'(x)$, where $x \in \mathcal{O}_L$ and f is the minimal polynomial of x over K.

REMARK B.2.25. It is important to point out that, in some references used in this book, such as [**31**] for example, $\mathfrak{d}_{L/K}$ denotes the discriminant ideal and $\mathcal{D}_{L/K}$ denotes the different ideal. □

We then have the following result.

THEOREM B.2.26. *Let L/K be an extension of number fields of degree n. Then the following properties hold:*

(1) *A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ ramifies in L if and only if $\mathfrak{p}$ divides $\mathcal{D}_{L/K}$. In particular, if $K = \mathbb{Q}$, p ramifies in L if and only if $p \mid \mathrm{disc}(L)$;*

(2) *let $\alpha \in \mathcal{O}_K$ such that $L = K(\alpha)$, with minimal polynomial f over K. Then*

$$D(1, \theta, \ldots, \theta^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(f'(\alpha)).$$

In particular, $\mathcal{D}_{L/K} | (N_{L/K}(f'(\alpha)))$.

(3) *the prime ideals of $\mathcal{O}_L$ which divide $\mathfrak{d}_{L/K}$ are exactly those who lie above ideals of $\mathcal{O}_K$ which ramify in L;*

(4) *$\mathcal{N}_{L/K}(\mathfrak{d}_{L/K}) = \mathcal{D}_{L/K}$. In particular, $N_{L/\mathbb{Q}}(\mathfrak{d}_{L/\mathbb{Q}}) = \mathrm{disc}(L)$.*

See [**43**, Section 13.2] for example.

EXAMPLE B.2.27. Let $L = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is a non-zero square-free integer. Then it readily follows from Example B.2.2 (1) that $\mathrm{disc}(L) = d$ if $d \equiv 1[4]$ and $4d$ otherwise. □

The following result is particularly useful to compute the ring of integers in some cases.

PROPOSITION B.2.28. *Let L and M be two number fields. Assume that $L/\mathbb{Q}$ and $M/\mathbb{Q}$ are linearly disjoint, and that* $\mathrm{disc}(L)$ *and* $\mathrm{disc}(M)$ *are coprime. Then $\mathcal{O}_{LM}$ is a generated as an abelian group by the elements*

$$xy, \ x \in \mathcal{O}_L, y \in \mathcal{O}_M.$$

Moreover, if $(e_1, \dots, e_n)$ *is a* $\mathbb{Z}$*-basis of* $\mathcal{O}_L$ *and* $(f_1, \dots, f_m)$ *is a* $\mathbb{Z}$*-basis of* $\mathcal{O}_M$*, then the elements*

$$e_i f_j, i = 1, \dots, n, j = 1, \dots, m$$

form a $\mathbb{Z}$*-basis of* $\mathcal{O}_{LM}$*.*

Proof. The first point is just a particular case of [**15**, (2.13)]. To prove the second part, notice that the first point shows that the elements

$$e_i f_j, i = 1, \dots, n, j = 1, \dots, m$$

span $\mathcal{O}_{LM}$ as an abelian group. It remains to prove that they are linearly independent over $\mathbb{Z}$ or, which is equivalent, over $\mathbb{Q}$. But this comes from the fact that $L/\mathbb{Q}$ and $M/\mathbb{Q}$ are linearly disjoint, noticing that $(e_1, \dots, e_n)$ and $(f_1, \dots, f_m)$ are also $\mathbb{Q}$-bases of L and M respectively. □

We now give a proposition which partially describes the ramification in a Kummer extension.

PROPOSITION B.2.29. *Assume that* $\mu_n \subset k$*, and let* $L = k(\sqrt[n]{d})$ *be a cyclic extension of* k *of degree* n*, where* $d \in \mathcal{O}_k \setminus \{0\}$*. Then the following properties hold:*

(1) *the prime ideals of* $\mathcal{O}_k$ *which eventually ramify are those which divide* d *or* n*;*

(2) *let* $\mathfrak{p} \mid d$*. If* $n_\mathfrak{p}(d)$ *is not a multiple of* n*, then* $\mathfrak{p}$ *ramifies. If moreover* $n_\mathfrak{p}(d)$ *and* n *are coprime, then* $\mathfrak{p}$ *totally ramifies.*

(3) *assume that* $\mathfrak{p} \mid d$ *and* $\mathfrak{p} \nmid n$*. Then* $\mathfrak{p}$ *ramifies (resp. totally ramifies) if and only if* $n_\mathfrak{p}(d)$ *is a not multiple of* n *(resp.* $n_\mathfrak{p}(d)$ *and* n *are coprime);*

(4) *assume that* n *is prime, and let* $\mathfrak{p} \nmid n$*. Then* $\mathfrak{p}$ *ramifies if and only if* $n_\mathfrak{p}(d)$ *is not a multiple of* n*. In this case, it totally ramifies.*

Proof. Let $\alpha = \sqrt[n]{d}$. The minimal polynomial f of α over k is $X^n - d$, whose discriminant is

$$\operatorname{disc}(f) = \pm N_{k(\alpha)/k}(f'(\alpha)) = \pm n^n d^n.$$

Now if $\mathfrak{p}$ ramifies, it divides the discriminant ideal $\mathcal{D}_{L/k}$ by Theorem B.2.26 (1). But $\mathcal{D}_{L/K} \mid \operatorname{disc}(f)$ by Theorem B.2.26 (2), and we get (1).

Let $\mathfrak{p} \mid d$ and let $r = gcd(n, n_\mathfrak{p}(d))$. Write $n = rm, n_\mathfrak{p}(d) = rs$, where and m and s are coprime. Notice that we have $r \leq n$ by definition. Let e the ramification index of $\mathfrak{p}$ in L. Since $\alpha^n = d$, comparing valuations with respect to any prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$, we get that $nn_\mathfrak{P}(\alpha) = en_\mathfrak{p}(d)$. Thus, we have $mn_\mathfrak{P}(\alpha) = es$ and therefore $m \mid e$ since m and s are coprime. Assume that $n_\mathfrak{p}(d)$ is not a multiple of n. Then we cannot have $r = n$ and therefore $m > 1$. Since $m > 1$, we have $e > 1$, hence $\mathfrak{p}$ ramifies. Moreover, if $n_\mathfrak{p}(d)$ and n are coprime, then $m = n$ and thus $n \mid e$. Since $e < n$, this means that $e = n$ and therefore, $\mathfrak{p}$ totally ramifies in this case, hence (2).

We now proceed to show (3). By Lemma B.2.5, there exists $c \in k$ such that $n_\mathfrak{p}(c) = -s$ and $n_\mathfrak{q}(c) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}$. It follows that $n_\mathfrak{p}(dc^r) = n_\mathfrak{p}(d) - rs = 0$, and that $n_\mathfrak{q}(dc^r) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}$. In other words, dc^r is an element of $\mathcal{O}_k$ which is not divisible by $\mathfrak{p}$.

Assume that $\mathfrak{p} \nmid n$. In particular, $\mathfrak{p} \nmid r$. Applying (1) to $k(\sqrt[n]{dc^r})$ shows that $\mathfrak{p}$ does not ramify in $k(\sqrt[n]{d})/k$. Now assume that $n_\mathfrak{p}(d)$ is a multiple of n. Hence

$r = gcd(n, n_{\mathfrak{p}}(d)) = n$, and $\mathfrak{p}$ does not ramify in L/k. By (2), if $n_{\mathfrak{p}}(d)$ is a multiple of n, then $\mathfrak{p}$ ramifies in L/k. Therefore, $\mathfrak{p}$ ramifies if and only if $n_{\mathfrak{p}}(d)$ is not a multiple of n. In this case, if $n_{\mathfrak{p}}(d)$ and n are not coprime, then $r \geq 2$ and $k(\sqrt[r]{d})/k$ is a non-trivial subextension of L/k in which $\mathfrak{p}$ does not ramify. Hence, $\mathfrak{p}$ ramifies but does not totally ramify in L/k. This proves (3).

Finally, if n is prime, then $n_{\mathfrak{p}}(d)$ is not a multiple of n if and only if $n_{\mathfrak{p}}(d)$ and n are coprime. Point (4) then follows from the previous points. This concludes the proof. □

We end this section by giving a list of results which allow us to compute the different ideal.

THEOREM B.2.30. *Let $K \subset L_1 \subset L_2$ be a tower of number fields. Then we have*

$$\mathfrak{d}_{L_2/K} = \mathfrak{d}_{L_2/L_1}\mathfrak{d}_{L_1/K}.$$

See [**31**, Theorem 3.12.3] for a proof.

The next result shows that the part of the different ideal corresponding to tame ramification is perfectly understood.

THEOREM B.2.31. *Let L/K be an extension of number fields. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be a ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then the following properties hold:*

(1) $n_{\mathfrak{P}}(\mathfrak{d}_{L/K}) = e_{\mathfrak{P}|\mathfrak{p}} - 1$ *if* $\mathfrak{p} \nmid e_{\mathfrak{P}|\mathfrak{p}}$;
(2) $n_{\mathfrak{P}}(\mathfrak{d}_{L/K}) > e_{\mathfrak{P}|\mathfrak{p}} - 1$ *if* $\mathfrak{p} \mid e_{\mathfrak{P}|\mathfrak{p}}$.

See [**31**, Theorem 3.12.9] for a proof.

We now explain how to deal with the case of wild ramification when L/K is a Galois extension of number fields with Galois group G. First, we need to define an appropriate filtration of subgroups of G.

DEFINITION B.2.32. Let L/K be a Galois extension of number fields with Galois group G. For any prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, the subgroup

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

is called the **decomposition group of $\mathfrak{P}$**.

For all $n \geq 0$, the **$n-$th ramification group of $\mathfrak{P}$** is the subgroup of G defined by

$$G_n(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\alpha) - \alpha \in \mathfrak{P}^{n+1} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

This is in fact a subgroup of $G_{\mathfrak{P}}$. Indeed, if $\sigma \in G_n(\mathfrak{P})$, then for all $\alpha \in \mathfrak{P}$, we have

$$\sigma(\alpha) \in \mathfrak{P} + \mathfrak{P}^{n+1} \subset \mathfrak{P}.$$

We then have $\sigma(\mathfrak{P}) \subset \mathfrak{P}$, which is equivalent to $\sigma(\mathfrak{P}) = \mathfrak{P}$ by maximality of $\sigma(\mathfrak{P})$. This means that $\sigma \in G_{\mathfrak{P}}$.

Finally, notice that for all $n \geq 0$, $G_n(\mathfrak{P})$ is a subgroup of $G_{n-1}(\mathfrak{P})$ (with the convention $G_{-1}(\mathfrak{P}) = G_{\mathfrak{P}}$).

The interest of this filtration is given by the following theorem.

THEOREM B.2.33. *Let L/K be a Galois extension of number fields. For any prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, the groups $G_n(\mathfrak{P})$ are trivial for a sufficiently large n, and we have*

$$n_{\mathfrak{P}}(\mathfrak{d}_{L/K}) = \sum_{n\geq 0}(|G_n(\mathfrak{P})| - 1).$$

We let the reader refer to [**30**, Theorem 1.54] for a proof.

B.3. Absolute values on number fields and completion

We start by describing the set of absolute values on a given number field.

Let K be a number field. Any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies above a unique prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$. We will say that $\mathfrak{p}$ lies above the prime p, and we will denote by $e_{\mathfrak{p}|p}$ and $f_{\mathfrak{p}|p}$ the corresponding ramification index and residual degree.

We then set

$$\upsilon_{\mathfrak{p}}: \begin{array}{c} K \longrightarrow \mathbb{R}^+ \\ x \longmapsto p^{-\frac{n_{\mathfrak{p}}(x)}{e_{\mathfrak{p}|p}}}. \end{array}$$

This is a non-trivial discrete absolute value on K, which extends the p-adic valuation υ_p of $\mathbb{Q}$.

REMARKS B.3.1.

(1) If $\mathfrak{p}$ is principal, generated by π, then π is a local parameter for $\upsilon_{\mathfrak{p}}$.
(2) One may show that the residue field of $\upsilon_{\mathfrak{p}}$ is isomorphic to $\kappa(\mathfrak{p})$.

□

Let $\sigma : K \longrightarrow \mathbb{C}$ be a $\mathbb{Q}$-embedding of K into $\mathbb{C}$. If $\sigma(K) \subset \mathbb{R}$, we call σ a **real** embedding and we set

$$\upsilon_{\sigma}: \begin{array}{c} K \longrightarrow \mathbb{R}^+ \\ x \longmapsto |\sigma(x)|, \end{array}$$

where $|\cdot|$ denotes the classical absolute value of $\mathbb{R}$.

If $\sigma(K) \not\subset \mathbb{R}$, we call σ a **complex** embedding. We will say that two complex embeddings σ_1, σ_2 are **conjugate** if $\sigma_2(x) = \overline{\sigma_1(x)}$ for all $x \in K$, where $^-$ denotes the complex conjugation. If σ is a complex embedding, we set

$$\upsilon_{\sigma}: \begin{array}{c} K \longrightarrow \mathbb{R}^+ \\ x \longmapsto |\sigma(x)|, \end{array}$$

where $|\cdot|$ denotes the modulus of a complex number.

In both cases, υ_σ is an archimedean valuation.

DEFINITION B.3.2. The absolute value $\upsilon_{\mathfrak{p}}$ on K is called the **$\mathfrak{p}$-adic absolute value**.

A place represented by an absolute value $\upsilon_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ is called a **finite** place.

A place represented by an absolute value υ_σ for some real (resp. complex) embedding is called a **real** (resp. **complex**) place.

We then have the following result.

THEOREM B.3.3. *Let K be a number field. Then the set of places of K is represented by the following absolute absolute values, which are pairwise non-equivalent:*

(1) *the absolute values $v_{\mathfrak{p}}$, where $\mathfrak{p}$ describes the set of prime ideals of $\mathcal{O}_K$;*

(2) *the absolute values v_σ, where σ describes the set of real embeddings of K;*

(3) *the absolute values v_σ, where σ describes a maximal set of pairwise non-conjugate complex embeddings of K.*

See [**51**], Lemmas 16 and 17.

Notice now that if L/K is an extension of number fields, and $\mathfrak{P} \mid \mathfrak{p}$, then the restriction of $v_{\mathfrak{P}}$ to K is $v_{\mathfrak{p}}$.

Indeed, it readily follows from the definitions that we have

$$n_{\mathfrak{P}}(x) = e_{\mathfrak{p}|\mathfrak{P}} n_{\mathfrak{p}}(x) \text{ for all } x \in K,$$

as well as

$$e_{\mathfrak{P}|p} = e_{\mathfrak{p}|p} e_{\mathfrak{P}|\mathfrak{p}}.$$

The claim follows easily. Thus, the following result makes sense.

LEMMA B.3.4. *Let L/K be a extension of number fields. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{P}$. Then we have*

$$e_{v_{\mathfrak{P}}|v_{\mathfrak{p}}} = e_{\mathfrak{P}|\mathfrak{p}} \quad \textit{and} \quad f_{v_{\mathfrak{P}}|v_{\mathfrak{p}}} = f_{\mathfrak{P}|\mathfrak{p}}.$$

Proof. If $\pi_{\mathfrak{p}}$ is a local parameter of $v_{\mathfrak{p}}$ and $\pi_{\mathfrak{P}}$ is a local parameter of $v_{\mathfrak{P}}$, we have

$$n_{\mathfrak{P}}(\pi_{\mathfrak{p}}) = e_{\mathfrak{P}|\mathfrak{p}} n_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = e_{\mathfrak{P}|\mathfrak{p}} = n_{\mathfrak{P}}(\pi_{\mathfrak{P}}^{e_{\mathfrak{P}|\mathfrak{p}}}),$$

so that $\pi_{\mathfrak{P}} = u\pi_{\mathfrak{P}}^{e_{\mathfrak{P}|\mathfrak{p}}}, u \in \mathcal{O}_{v_{\mathfrak{P}}}^{\times}$. By Remark B.1.14, we get the equality

$$e_{v_{\mathfrak{P}}|v_{\mathfrak{p}}} = e_{\mathfrak{P}|\mathfrak{p}}.$$

The second equality comes from the fact that the residue fields of $v_{\mathfrak{p}}$ and $v_{\mathfrak{P}}$ are respectively $\kappa(\mathfrak{p})$ and $\kappa(\mathfrak{P})$. □

To end this section, we would like to relate number fields and local fields via their completions with respect to a valuation. Let K be a number field. Notice that equivalent absolute values give rise to canonically isomorphic completions. If v is a place of K, we will write K_v for the completion of K with respect to any valuation representing this place.

If v is a real place, then $K_v \simeq \mathbb{R}$, and if v is a complex place, we have $K_v \simeq \mathbb{C}$.

Now assume that v is a finite place, and let $\mathfrak{p}$ the corresponding prime ideal of $\mathcal{O}_K$. We will denote by $K_{\mathfrak{p}}$ the corresponding completion. Since $K_{\mathfrak{p}}$ is complete for a non-trivial discrete absolute value with finite residue field $\kappa(\mathfrak{p})$, this is a local field.

Let L/K be an extension of number fields. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be an ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Since $v_{\mathfrak{P}}$ extends $v_{\mathfrak{p}}$, we get an extension $(L_{\mathfrak{P}}, v_{\mathfrak{P}})/(K_{\mathfrak{p}}, v_{\mathfrak{p}})$ of local fields.

Since completion preserves the ramification index and the residual degree, this extension has ramification index $e_{\mathfrak{P}|\mathfrak{p}}$ and residual degree $f_{\mathfrak{P}|\mathfrak{p}}$. In particular, we have the following result.

PROPOSITION B.3.5. *Let L/K be an extension of number fields. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be an ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then we have*

$$[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}.$$

To conclude this appendix, we take a look to the Galois case. The only thing which does not derive from the previous result results in the next proposition is the equality $L_{\mathfrak{P}} = LK_{\mathfrak{p}}$, which is proved in [**44**] Chapter II, §3.

PROPOSITION B.3.6. *Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$, and let $\mathfrak{P}$ be any ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then $L_{\mathfrak{P}} = LK_{\mathfrak{p}}$ (in the completion of an algebraic closure of $k_{\mathfrak{p}}$). In particular, it does not depend on the choice of $\mathfrak{P}$, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois, and its Galois group identifies to a subgroup of $\mathrm{Gal}(L/K)$ of order $e_{\mathfrak{p}} f_{\mathfrak{p}}$.*

Finally, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified, resp. ramified, resp. totally ramified if and only if $\mathfrak{p}$ is.

REMARK B.3.7. In particular, if L/K is cyclic, so is $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. □