Introduction to Algebraic Number Theory

F. Oggier

A few words

These are lecture notes for the class on introduction to algebraic number theory, given at NTU from January to April 2009 and 2010.

These lectures notes follow the structure of the lectures given by C. Wüthrich at EPFL. I would like to thank Christian for letting me use his notes as basic material.

I also would like to thank Martianus Frederic Ezerman, Nikolay Gravin and LIN Fuchun for their comments on these lecture notes.

At the end of these notes can be found a short bibliography of a few classical books relevant (but not exhaustive) for the topic: [3, 6] are especially friendly for a first reading, [1, 2, 5, 7] are good references, while [4] is a reference for further reading.

Contents

Chapter 1

Algebraic Numbers and Algebraic Integers

1.1 Rings of integers

We start by introducing two essential notions: number field and algebraic integer.

Definition 1.1. A number field is a finite field extension K of $\mathbb{Q}$, i.e., a field which is a $\mathbb{Q}$-vector space of finite dimension. We note this dimension $[K : \mathbb{Q}]$ and call it the degree of K.

Examples 1.1. 1. The field

$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$$

is a number field. It is of degree 2 over $\mathbb{Q}$. Number fields of degree 2 over $\mathbb{Q}$ are called quadratic fields. More generally, $\mathbb{Q}[X]/f(X)$ is a number field if f is irreducible. It is of degree the degree of the polynomial f.

2. Let ζ_n be a primitive nth root of unity. The field $\mathbb{Q}(\zeta_n)$ is a number field called cyclotomic field.

3. The fields $\mathbb{C}$ and $\mathbb{R}$ are not number fields.

Let K be a number field of degree n. If $\alpha \in K$, there must be a $\mathbb{Q}$-linear dependency among $\{1, \alpha, \ldots, \alpha^n\}$, since K is a $\mathbb{Q}$-vector space of dimension n. In other words, there exists a polynomial $f(X) \in \mathbb{Q}[X]$ such that $f(X) = 0$. We call α an algebraic number.

Definition 1.2. An algebraic integer in a number field K is an element $\alpha \in K$ which is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

Example 1.2. Since $X^2-2=0$, $\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ is an algebraic integer. Similarly, $i\in\mathbb{Q}(i)$ is an algebraic integer, since $X^2+1=0$. However, an element $a/b\in\mathbb{Q}$ is not an algebraic integer, unless b divides a.

Now that we have the concept of an algebraic integer in a number field, it is natural to wonder whether one can compute the set of all algebraic integers of a given number field. Let us start by determining the set of algebraic integers in $\mathbb{Q}$.

Definition 1.3. The minimal polynomial f of an algebraic number α is the monic polynomial in $\mathbb{Q}[X]$ of smallest degree such that $f(\alpha)=0$.

Proposition 1.1. *The minimal polynomial of α has integer coefficients if and only if α is an algebraic integer.*

Proof. If the minimal polynomial of α has integer coefficients, then by definition (Definition 1.2) α is algebraic.

Now let us assume that α is an algebraic integer. This means by definition that there exists a monic polynomial $f\in\mathbb{Z}[X]$ such that $f(\alpha)=0$. Let $g\in\mathbb{Q}[X]$ be the minimal polyonial of α. Then $g(X)$ divides $f(X)$, that is, there exists a monic polynomial $h\in\mathbb{Q}[X]$ such that

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

(Note that h is monic because f and g are). We want to prove that $g(X)$ actually belongs to $\mathbb{Z}[X]$. Assume by contradiction that this is not true, that is, there exists at least one prime p which divides one of the denominators of the coefficients of g. Let $u>0$ be the smallest integer such that p^ug does not have anymore denominators divisible by p. Since h may or may not have denominators divisible by p, let $v\geq 0$ be the smallest integer such that p^vh has no denominator divisible by p. We then have

$$p^ug(X)p^vh(X)=p^{u+v}f(X).$$

The left hand side of this equation does not have denominators divisible by p anymore, thus we can look at this equation modulo p. This gives

$$p^ug(X)p^vh(X)\equiv 0\in\mathbb{F}_p[X],$$

where $\mathbb{F}_p$ denotes the finite field with p elements. This give a contradiction, since the left hand side is a product of two non-zero polynomials (by minimality of u and v), and $\mathbb{F}_p[X]$ does not have zero divisor. □

Corollary 1.2. *The set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.*

Proof. Let $\frac{a}{b}\in\mathbb{Q}$. Its minimal polynomial is $X-\frac{a}{b}$. By the above proposition, $\frac{a}{b}$ is an algebraic integer if and only $b=\pm 1$. □

Definition 1.4. The set of algebraic integers of a number field K is denoted by $\mathcal{O}_K$. It is usually called the ring of integers of K.

The fact that $\mathcal{O}_K$ is a ring is not obvious. In general, if one takes a, b two algebraic integers, it is not straightforward to find a monic polynomial in $\mathbb{Z}[X]$ which has $a+b$ as a root. We now proceed to prove that $\mathcal{O}_K$ is indeed a ring.

Theorem 1.3. *Let K be a number field, and take $\alpha \in K$. The two statements are equivalent:*

1. *α is an algebraic integer.*
2. *The Abelian group $\mathbb{Z}[\alpha]$ is finitely generated (a group G is finitely generated if there exist finitely many elements $x_1, ..., x_s \in G$ such that every $x \in G$ can be written in the form $x = n_1x_1 + n_2x_2 + ... + n_sx_s$ with integers $n_1, ..., n_s$).*

Proof. Let α be an algebraic integer, and let m be the degree of its minimal polynomial, which is monic and with coefficients in $\mathbb{Z}$ by Proposition 1.1. Since all α^u with $u \geq m$ can be written as $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{m-1}$, we have that

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \ldots \oplus \mathbb{Z}\alpha^{m-1}$$

and $\{1, \alpha, \ldots, \alpha^{m-1}\}$ generate $\mathbb{Z}[\alpha]$ as an Abelian group. Note that for this proof to work, we really need the minimal polynomial to have coefficients in $\mathbb{Z}$, and to be monic!

Conversely, let us assume that $\mathbb{Z}[\alpha]$ is finitely generated, with generators $a_1, \ldots, a_m$, where $a_i = f_i(\alpha)$ for some $f_i \in \mathbb{Z}[X]$. In order to prove that α is an algebraic integer, we need to find a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. Let N be an integer such that $N > \deg f_i$ for $i = 1, \ldots, m$. We have that

$$\alpha^N = \sum_{j=1}^{m} b_j a_j, \ b_j \in \mathbb{Z}$$

that is

$$\alpha^N - \sum_{j=1}^{m} b_j f_j(\alpha) = 0.$$

Let us thus choose

$$f(X) = X^N - \sum_{j=1}^{m} b_j f_j(X).$$

Clearly $f \in \mathbb{Z}[X]$, it is monic by the choice of $N > \deg f_i$ for $i = 1, \ldots, m$, and finally $f(\alpha) = 0$. So α is an algebraic integer. □

Example 1.3. We have that

$$\mathbb{Z}[1/2] = \left\{ \frac{a}{b} \mid b \text{ is a power of } 2 \right\}$$

is not finitely generated, since $\frac{1}{2}$ is not an algebraic integer. Its minimal polynomial is $X - \frac{1}{2}$.

Corollary 1.4. *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

Proof. Let $\alpha, \beta \in \mathcal{O}_K$. The above theorem tells us that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, thus so is $\mathbb{Z}[\alpha, \beta]$. Now, $\mathbb{Z}[\alpha, \beta]$ is a ring, thus in particular $\alpha \pm \beta$ and $\alpha\beta \in \mathbb{Z}[\alpha, \beta]$. Since $\mathbb{Z}[\alpha \pm \beta]$ and $\mathbb{Z}[\alpha\beta]$ are subgroups of $\mathbb{Z}[\alpha, \beta]$, they are finitely generated. By invoking again the above theorem, $\alpha \pm \beta$ and $\alpha\beta \in \mathcal{O}_K$. □

Corollary 1.5. *Let K be a number field, with ring of integers $\mathcal{O}_K$. Then $\mathbb{Q}\mathcal{O}_K = K$.*

Proof. It is clear that if $x = b\alpha \in \mathbb{Q}\mathcal{O}_K$, $b \in \mathbb{Q}$, $\alpha \in \mathcal{O}_K$, then $x \in K$.

Now if $\alpha \in K$, we show that there exists $d \in \mathbb{Z}$ such that $\alpha d \in \mathcal{O}_K$ (that is $\alpha d = \beta \in \mathcal{O}_K$, or equivalently, $\alpha = \beta/d$). Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α. Choose d to be the least common multiple of the denominators of the coefficients of $f(X)$, then (recall that f is monic!)

$$d^{\deg(f)} f\left(\frac{X}{d}\right) = g(X),$$

and $g(X) \in \mathbb{Z}[X]$ is monic, with αd as a root. Thus $\alpha d \in \mathcal{O}_K$. □

1.2 Norms and Traces

Definition 1.5. Let L/K be a finite extension of number fields. Let $\alpha \in L$. We consider the multiplication map by α, denoted by μ_α, such that

$$\begin{aligned} \mu_\alpha : \quad L &\to \quad L \\ x &\mapsto \quad \alpha x. \end{aligned}$$

This is a K-linear map of the K-vector space L into itself (or in other words, an endomorphism of the K-vector space L). We call the norm of α the determinant of μ_α, that is

$$\mathrm{N}_{L/K}(\alpha) = \det(\mu_\alpha) \in K,$$

and the trace of α the trace of μ_α, that is

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(\mu_\alpha) \in K.$$

Note that the norm is multiplicative, since

$$\mathrm{N}_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha)\det(\mu_\beta) = \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\beta)$$

while the trace is additive:

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}(\mu_{\alpha+\beta}) = \mathrm{Tr}(\mu_\alpha+\mu_\beta) = \mathrm{Tr}(\mu_\alpha)+\mathrm{Tr}(\mu_\beta) = \mathrm{Tr}_{L/K}(\alpha)+\mathrm{Tr}_{L/K}(\beta).$$

In particular, if n denotes the degree of L/K, we have that

$$\mathrm{N}_{L/K}(a\alpha) = a^n \mathrm{N}_{L/K}(\alpha),\ \mathrm{Tr}_{L/K}(a\alpha) = a\mathrm{Tr}_{L/K}(\alpha),\ a \in K.$$

Indeed, the matrix of μ_a is given by a diagonal matrix whose coefficients are all a when $a \in K$.

Recall that the characteristic polynomial of $\alpha \in L$ is the characteristic polynomial of μ_α, that is

$$\chi_{L/K}(X) = \det(XI - \mu_\alpha) \in K[X].$$

This is a monic polynomial of degree $n = [L : K]$, the coefficient of X^{n-1} is $-\mathrm{Tr}_{L/K}(\alpha)$ and its constant term is $\pm \mathrm{N}_{L/K}(\alpha)$.

Example 1.4. Let L be the quadratic field $\mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$, and take $\alpha \in \mathbb{Q}(\sqrt{2})$. In order to compute μ_α, we need to fix a basis of $\mathbb{Q}(\sqrt{2})$ as $\mathbb{Q}$-vector space, say

$$\{1, \sqrt{2}\}.$$

Thus, α can be written $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. By linearity, it is enough to compute μ_α on the basis elements:

$$\mu_\alpha(1) = a + b\sqrt{2},\ \mu_\alpha(\sqrt{2}) = (a + b\sqrt{2})\sqrt{2} = a\sqrt{2} + 2b.$$

We now have that

$$\begin{pmatrix} 1, & \sqrt{2} \end{pmatrix} \underbrace{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}}_{M} = \begin{pmatrix} a + b\sqrt{2}, & 2b + a\sqrt{2} \end{pmatrix}$$

and M is the matrix of μ_α in the chosen basis. Of course, M changes with a change of basis, but the norm and trace of α are independent of the basis. We have here that

$$\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = a^2 - 2b^2,\ \mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = 2a.$$

Finally, the characteristic polynomial of μ_α is given by

$$\begin{aligned} \chi_{L/K}(X) &= \det\left(XI - \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\right) \\ &= \det\begin{pmatrix} X - a & -b \\ -2b & X - a \end{pmatrix} \\ &= (X - a)(X - a) - 2b^2 \\ &= X^2 - 2aX + a^2 - 2b^2. \end{aligned}$$

We recognize that the coefficient of X is indeed the trace of α with a minus sign, while the constant coefficient is its norm.

We now would like to give another equivalent definition of the trace and norm of an algebraic integer α in a number field K, based on the different roots of the minimal polynomial of α. Since these roots may not belong to K, we first need to introduce a bigger field which will contain all the roots of the polynomials we will consider.

Definition 1.6. The field $\bar{F}$ is called an algebraic closure of a field F if all the elements of $\bar{F}$ are algebraic over F and if every polynomial $f(X) \in F[X]$ splits completely over $\bar{F}$.

We can think that $\bar{F}$ contains all the elements that are algebraic over F, in that sense, it is the largest algebraic extension of F. For example, the field of complex numbers $\mathbb{C}$ is the algebraic closure of the field of reals $\mathbb{R}$ (this is the fundamental theorem of algebra). The algebraic closure of $\mathbb{Q}$ is denoted by $\bar{\mathbb{Q}}$, and $\bar{\mathbb{Q}} \subset \mathbb{C}$.

Lemma 1.6. *Let K be number field, and let $\bar{K}$ be its algebraic closure. Then an irreducibe polynomial in $K[X]$ cannot have a multiple root in $\bar{K}$.*

Proof. Let $f(X)$ be an irreducible polynomial in $K[X]$. By contradiction, let us assume that $f(X)$ has a multiple root α in $\bar{K}$, that is $f(X) = (X-\alpha)^m g(X)$ with $m \geq 2$ and $g(\alpha) \neq 0$. We have that the formal derivative of $f'(X)$ is given by

$$\begin{aligned} f'(X) &= m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X) \\ &= (X-\alpha)^{m-1}(mg(X) + (X-\alpha)g'(X)), \end{aligned}$$

and therefore $f(X)$ and $f'(X)$ have $(X-\alpha)^{m-1}$, $m \geq 2$, as a common factor in $\bar{K}[X]$. In other words, α is root of both $f(X)$ and $f'(X)$, implying that the minimal polynomial of α over K is a common factor of $f(X)$ and $f'(X)$. Now since $f(X)$ is irreducible over $K[X]$, this common factor has to be $f(X)$ itself, implying that $f(X)$ divides $f'(X)$. Since $\deg(f'(X)) < \deg(f(X))$, this forces $f'(X)$ to be zero, which is not possible with K of characteristic 0. □

Thanks to the above lemma, we are now able to prove that an extension of number field of degree n can be embedded in exactly n different ways into its algebraic closure. These n embeddings are what we need to redefine the notions of norm and trace. Let us first recall the notion of field monomorphism.

Definition 1.7. Let L_1, L_2 be two field extensions of a field K. A field monomorphism σ from L_1 to L_2 is a field homomorphism, that is a map from L_1 to L_2 such that, for all $a, b \in L_1$,

$$\begin{aligned} \sigma(ab) &= \sigma(a)\sigma(b) \\ \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(1) &= 1 \\ \sigma(0) &= 0. \end{aligned}$$

A field homomorphism is automatically an injective map, and thus a field monomorphism. It is a field K-monomorphism if it fixes K, that is, if $\sigma(c) = c$ for all $c \in K$.

Example 1.5. We consider the number field $K = \mathbb{Q}(i)$. Let $x = a + ib \in \mathbb{Q}(i)$. If σ is field $\mathbb{Q}$-homomorphism, then $\sigma(x) = a + \sigma(i)b$ since it has to fix $\mathbb{Q}$. Furthermore, we need that

$$\sigma(i)^2 = \sigma(i^2) = -1,$$

so that $\sigma(i) = \pm i$. This gives us exactly two $\mathbb{Q}$-monomorphisms of K into $\bar{K} \subset \mathbb{C}$, given by:

$$\sigma_1 : a + ib \mapsto a + ib,\ \sigma_2 : a + ib \mapsto a - ib,$$

that is the identity and the complex conjugation.

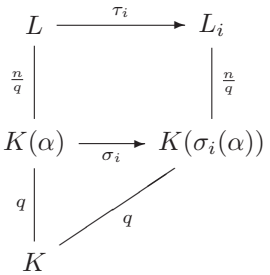
Proposition 1.7. *Let K be a number field, L be a finite extension of K of degree n, and $\bar{K}$ be an algebraic closure of K. There are n distinct K-monomorphisms of L into $\bar{K}$.*

Proof. This proof is done in two steps. In the first step, the claim is proved in the case when $L = K(\alpha)$, $\alpha \in L$. The second step is a proof by induction on the degree of the extension L/K in the general case, which of course uses the first step. The main idea is that if $L \neq K(\alpha)$ for some $\alpha \in L$, then one can find such intermediate extension, that is, we can consider the tower of extensions $K \subset K(\alpha) \subset L$, where we can use the first step for $K(\alpha)/K$ and the induction hypothesis for $L/K(\alpha)$.

Step 1. Let us consider $L = K(\alpha)$, $\alpha \in L$ with minimal polynomial $f(X) \in K[X]$. It is of degree n and thus admits n roots $\alpha_1, \ldots, \alpha_n$ in $\bar{K}$, which are all distinct by Lemma 1.6. For $i = 1, \ldots, n$, we thus have a K-monomorphism $\sigma_i : L \to \bar{K}$ such that $\sigma_i(\alpha) = \alpha_i$.

Step 2. We now proceed by induction on the degree n of L/K. Let $\alpha \in L$ and consider the tower of extensions $K \subset K(\alpha) \subset L$, where we denote by q, $q > 1$, the degree of $K(\alpha)/K$. We know by the first step that there are q distinct K-monomomorphisms from $K(\alpha)$ to $\bar{K}$, given by $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, q$, where α_i are the q roots of the minimal polynomial of α.

Now the fields $K(\alpha)$ and $K(\sigma_i(\alpha))$ are isomorphic (the isomorphism is given by σ_i) and one can build an extension L_i of $K(\sigma_i(\alpha))$ and an isomorphism $\tau_i : L \to L_i$ which extends σ_i (that is, τ_i restricted to $K(\alpha)$ is nothing else than σ_i):



Now, since

$$[L_i : K(\sigma_i(\alpha))] = [L : K(\alpha)] = \frac{n}{q} < n,$$

we have by induction hypothesis that there are $\frac{n}{q}$ distinct $K(\sigma_i(\alpha))$-monomorphisms θ_{ij} of L_i into $\bar{K}$. Therefore, $\theta_{ij} \circ \tau_i$, $i = 1, \ldots, q$, $j = 1, \ldots, \frac{n}{q}$ provide n distinct K-monomorphisms of L into $\bar{K}$. □

Corollary 1.8. *A number field K of degree n over $\mathbb{Q}$ has n embeddings into $\mathbb{C}$.*

Proof. The proof is immediate from the proposition. It is very common to find in the literature expressions such as "let K be a number field of degree n, and $\sigma_1, \ldots, \sigma_n$ be its n embeddings", without further explanation. □

Definition 1.8. Let L/K be an extension of number fields, and let $\alpha \in L$. Let $\sigma_1, \ldots, \sigma_n$ be the n field K-monomorphisms of L into $\bar{K} \subset \mathbb{C}$ given by the above proposition. We call $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ the conjugates of α.

Proposition 1.9. *Let L/K be an extension of number fields. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of L into $\mathbb{C}$ which fix K. For all $\alpha \in L$, we have*

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \ \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Proof. Let $\alpha \in L$, with minimal polynomial $f(X) \in K[X]$ of degree m, and let $\chi_{K(\alpha)/K}(X)$ be its characteristic polynomial.

Let us first prove that $f(X) = \chi_{K(\alpha)/K}(X)$. Note that both polynomials are monic by definition. Now the K-vector space $K(\alpha)$ has dimension m, thus m is also the degree of $\chi_{K(\alpha)/K}(X)$. By Cayley-Hamilton theorem (which states that every square matrix over the complex field satisfies its own characteristic equation), we have that

$$\chi_{K(\alpha)/K}(\mu_\alpha) = 0.$$

Now since

$$\chi_{K(\alpha)/K}(\mu_\alpha) = \mu_{\chi_{K(\alpha)/K}(\alpha)},$$

(see Example 1.7), we have that α is a root of $\chi_{K(\alpha)/K}(X)$. By minimality of the minimal polynomial $f(X)$, $f(X) \mid \chi_{K(\alpha)/K}(X)$, but knowing that both polynomials are monic of same degree, it follows that

$$f(X) = \chi_{K(\alpha)/K}(X). \tag{1.1}$$

We now compute the matrix of μ_α in a K-basis of L. We have that

$$\{1, \alpha, \ldots, \alpha^{m-1}\}$$

is a K-basis of $K(\alpha)$. Let k be the degree $[L : K(\alpha)]$ and let $\{\beta_1, \ldots, \beta_k\}$ be a $K(\alpha)-$basis of L. The set $\{\alpha^i \beta_j\}$, $0 \leq i < m$, $1 \leq j \leq k$ is a K-basis of L. The multiplication μ_α by α can now be written in this basis as

$$\mu_\alpha = \underbrace{\begin{pmatrix} B & 0 & \ldots & 0 \\ 0 & B & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \ldots & B \end{pmatrix}}_{k \text{ times}}, \ B = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ a_0 & a_1 & \ldots & a_{m-1} \end{pmatrix}$$

where a_i, $i = 0, \ldots, m-1$ are the coefficients of the minimal polynomial $f(X)$ (in other words, B is the companion matrix of f). We conclude that

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \mathrm{N}_{K(\alpha)/K}(\alpha)^k, \\ \mathrm{Tr}_{L/K}(\alpha) &= k\mathrm{Tr}_{K(\alpha)/K}(\alpha), \\ \chi_{L/K}(X) &= (\chi_{K(\alpha)/K})^k = f(X)^k, \end{aligned}$$

where last equality holds by (1.1). Now we have that

$$\begin{aligned} f(X) &= (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_m) \in \bar{\mathbb{Q}}[X] \\ &= X^m - \sum_{i=1}^{m} \alpha_i X^{m-1} + \ldots \pm \prod_{i=1}^{m} \alpha_i \in \mathbb{Q}[X] \\ &= X^m - \mathrm{Tr}_{K(\alpha)/K}(\alpha) X^{m-1} + \ldots \pm \mathrm{N}_{K(\alpha)/K}(\alpha) \in \mathbb{Q}[X] \end{aligned}$$

where last equality holds by (1.1), so that

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \left(\prod_{i=1}^{m} \alpha_i \right)^k, \\ \mathrm{Tr}_{L/K}(\alpha) &= k \sum_{i=1}^{m} \alpha_i. \end{aligned}$$

To conclude, we know that the embeddings of $K(\alpha)$ into $\bar{\mathbb{Q}}$ which fix K are determined by the roots of α, and we know that there are exactly m distinct such roots (Lemma 1.6). We further know (see Proposition 1.7) that each of these embeddings can be extended into an embedding of L into $\bar{\mathbb{Q}}$ in exactly k ways. Thus

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \prod_{i=1}^{n} \sigma_i(\alpha), \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum_{i=1}^{n} \sigma_i(\alpha), \end{aligned}$$

which concludes the proof. □

Example 1.6. Consider the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. It has two embeddings

$$\sigma_1 : a + b\sqrt{2} \mapsto a + b\sqrt{2}, \ \sigma_2 : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Take the element $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Its two conjugates are $\sigma_1(\alpha) = \alpha = a + b\sqrt{2}$, $\sigma_2(\alpha) = a - b\sqrt{2}$, thus its norm is given by

$$\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 - 2b^2,$$

while its trace is

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha).$$

It of course gives the same answer as what we computed in Example 1.4.

Example 1.7. Consider again the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Take the element $\alpha = a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, whose characteristic polynomial is given by, say, $\chi(X) = p_0 + p_1X + p_2X^2$. Thus $\chi(\alpha) = p_0 + p_1(a + b\sqrt{2}) + p_2(a^2 + 2ab\sqrt{2} + 2b^2) = (p_0 + p_1a + p_2a^2 + p_2 2b^2) + (p_1b + p_2 2ab)\sqrt{2}$, and

$$\mu_{\chi(\alpha)} = \begin{pmatrix} p_0 + p_1a + p_2a^2 + p_2 2b^2 & 2bp_1 + 4p_2ab \\ p_1b + p_2 2ab & p_0 + p_1a + p_2a^2 + p_2 2b^2 \end{pmatrix}$$

(see Example 1.4). On the other hand, we have that

$$\chi(\mu_\alpha) = p_0 I + p_1 \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + p_2 \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}^2.$$

Thus we have that $\mu_{\chi(\alpha)} = \chi(\mu_\alpha)$.

Example 1.8. Consider the number field extensions $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{2})$. There are four embeddings of $\mathbb{Q}(i, \sqrt{2})$, given by

$$\begin{array}{lll} \sigma_1 : & i \mapsto i, & \sqrt{2} \mapsto \sqrt{2} \\ \sigma_2 : & i \mapsto -i, & \sqrt{2} \mapsto \sqrt{2} \\ \sigma_3 : & i \mapsto i, & \sqrt{2} \mapsto -\sqrt{2} \\ \sigma_4 : & i \mapsto -i, & \sqrt{2} \mapsto -\sqrt{2} \end{array}$$

We have that

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = \sigma_1(a + ib)\sigma_2(a + ib) = a^2 + b^2,\ a, b \in \mathbb{Q}$$

but

$$\begin{aligned} N_{\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}}(a + ib) &= \sigma_1(a + ib)\sigma_2(a + ib)\sigma_3(a + ib)\sigma_4(a + ib) \\ &= \sigma_1(a + ib)\sigma_2(a + ib)\sigma_1(a + ib)\sigma_2(a + ib) \\ &= \sigma_1(a + ib)^2\sigma_2(a + ib)^2 \\ &= (a^2 + b^2)^2 \end{aligned}$$

since $a, b \in \mathbb{Q}$.

Corollary 1.10. *Let K be a number field, and let $\alpha \in K$ be an algebraic integer. The norm and the trace of α belong to $\mathbb{Z}$.*

Proof. The characteristic polynomial $\chi_{K/\mathbb{Q}}(X)$ is a power of the minimal polynomial (see inside the proof of the above theorem), thus it belongs to $\mathbb{Z}[X]$. □

Corollary 1.11. *The norm $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ of an element α of $\mathcal{O}_K$ is equal to ± 1 if and only if α is a unit of $\mathcal{O}_K$.*

Proof. Let α be a unit of $\mathcal{O}_K$. We want to prove that its norm is ± 1. Since α is a unit, we have that by definition $1/\alpha \in \mathcal{O}_K$. Thus

$$1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathrm{N}_{K/\mathbb{Q}}(1/\alpha)$$

by multiplicativity of the norm. By the above corollary, both $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ and its inverse belong to $\mathbb{Z}$, meaning that the only possible values are ± 1.

Conversely, let us assume that $\alpha \in \mathcal{O}_K$ has norm ± 1, which means that the constant term of its minimal polynomial $f(X)$ is ± 1:

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots \pm 1.$$

Let us now consider $1/\alpha \in K$. We see that $1/\alpha$ is a root of the monic polynomial

$$g(X) = 1 + a_{n-1}X + \cdots \pm X^n,$$

with $g(X) \in \mathbb{Z}[X]$. Thus $1/\alpha$ is an algebraic integer. □

Let us prove a last result on the structure of the ring of integers. Recall that a group G is finitely generated if there exist finitely many elements $x_1, \ldots, x_s \in G$ such that every $x \in G$ can be written in the form $x = n_1x_1 + \ldots + n_sx_s$, with $n_1, \ldots, n_s$ integers. Such a group is called free if it is isomorphic to $\mathbb{Z}^r$, $r \geq 0$, called the rank of G. We now prove that $\mathcal{O}_K$ is not only a ring, but it is furthermore a free Abelian group of rank the degree of the corresponding number field.

Proposition 1.12. *Let K be a number field. Then $\mathcal{O}_K$ is a free Abelian group of rank $n = [K : \mathbb{Q}]$.*

Proof. We know by Corollary 1.5 that there exists a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of K with $\alpha_i \in \mathcal{O}_K$ for $i = 1, \ldots, n$ (take a basis of K with elements in K, and multiply the elements by the proper factors to obtain elements in $\mathcal{O}_K$ as explained in Corollary 1.5). Thus, an element $x \in \mathcal{O}_K$ can be written as

$$x = \sum_{i=1}^{n} c_i\alpha_i, \ c_i \in \mathbb{Q}.$$

Our goal is now to show that the denominators of c_i are bounded for all c_i and all $x \in \mathcal{O}_K$. To prove this, let us assume by contradiction that this is not the case, that is, that there exists a sequence

$$x_j = \sum_{i=1}^{n} c_{ij}\alpha_i, \ c_{ij} \in \mathbb{Q}$$

such that the greatest denominator of c_{ij}, $i = 1, \ldots, n$ goes to infinity when $j \to \infty$. Let us look at the norm of such an x_j. We know that $N_{K/\mathbb{Q}}(x_j)$ is the determinant of an $n \times n$ matrix with coefficients in $\mathbb{Q}[c_{ij}]$ (that is coefficients are $\mathbb{Q}$-linear combinations of c_{ij}). Thus the norm is a homogeneous polynomial

in c_{ij}, whose coefficients are determined by the field extension considered. Furthermore, it belongs to $\mathbb{Z}$ (Corollary 1.10). Since the coefficients are fixed and the norm is in $\mathbb{Z}$, the denominators of c_{ij} cannot grow indefinitely. They have to be bounded by a given constant B. Thus we have shown that

$$\mathcal{O}_K \subset \frac{1}{B} \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i.$$

Since the right hand side is a free Abelian group, $\mathcal{O}_K$ is free. Furthermore, $\mathcal{O}_K$ contains n elements which are linearly independent over $\mathbb{Q}$, thus the rank of $\mathcal{O}_K$ is n. □

Example 1.9. Let ζ_p be a primitive pth root of unity. One can show that the ring of integers of $\mathbb{Q}(\zeta_p)$ is

$$\mathbb{Z}[\zeta_p] = \mathbb{Z} \oplus \mathbb{Z}\zeta_p \cdots \oplus \mathbb{Z}\zeta_p^{p-2}.$$

Proposition 1.13. *Let K be a number field. Let $\alpha \in K$. If α is the zero of a monic polynomial f with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$. We say that $\mathcal{O}_K$ is integrally closed.*

Proof. Let us write $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$, with $a_i \in \mathcal{O}_K$. We know by the above proposition that $\mathcal{O}_K$ is a free abelian group which is finitely generated. Since

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_0,$$

we have that $\mathcal{O}_K[\alpha]$ is finitely generated as Abelian group. Thus $\mathbb{Z}[\alpha] \subset \mathcal{O}_K[\alpha]$ is also finitely generated, and α is an algebraic integer by Theorem 1.3. □

The main definitions and results of this chapter are

- Definition of a number field K of degree n and its ring of integers $\mathcal{O}_K$.
- Properties of $\mathcal{O}_K$: it is a ring with a $\mathbb{Z}$-basis of n elements, and it is integrally closed.
- The fact that K has n embeddings into $\mathbb{C}$.
- Definition of norm and trace, with their characterization as respectively product and sum of the conjugates.

Chapter 2

Ideals

For the whole chapter, K is a number field of degree n and $\mathcal{O} = \mathcal{O}_K$ is its ring of integers.

2.1 Introduction

Historically, experience with unique prime factorization of integers led mathematicians in the early days of algebraic number theory to a general intuition that factorization of algebraic integers into primes should also be unique. A likely reason for this misconception is the actual definition of what is a prime number. The familiar definition is that a prime number is a number which is divisible only by 1 and itself. Since units in $\mathbb{Z}$ are ± 1, this definition can be rephrased as: if $p = ab$, then one of a or b must be a unit. Equivalently over $\mathbb{Z}$, a prime number p satisfies that if $p|ab$, then $p|a$ or $p|b$. However, these two definitions are not equivalent anymore over general rings of integers. In fact, the second property is actually stronger, and if one can get a factorization with "primes" satisfying this property, then factorization will be unique, which is not the case for "primes" satisfying the first property. To distinguish these two definitions, we say in modern terminology that a number satisfying the first property is *irreducible*, while one satisfying the second property is *prime*.

Consider for example $\mathbb{Z}[\sqrt{-6}]$. We have that

$$6 = 2 \cdot 3 = -\sqrt{-6}\sqrt{-6}.$$

We get two factorizations into irreducibles (we have a factorization but it is not unique). However this is not a factorization into primes, since $\sqrt{-6}$ divides $2 \cdot 3$ but $\sqrt{-6}$ does not divide 2 and does not divide 3 either. So in the case where primes and irreducibles are different, we now have to think what we are looking for when we say factorization. When we attempt to factorize an element x in a domain D, we naturally mean proper factors a, b such that $x = ab$, and if either

of these factors can be further decomposed, we go on. That means, we look for writing

$$x = a_1 a_2 \dots a_n$$

into factors that cannot be reduced any further. The definition of irreducible captures what it means for the factorization to terminate: one of the term has to be a unit.

Thus what we are interested in is to understand the factorization into *irreducibles* inside rings of integers. Before starting, let us make a few more remarks. Note first that this factorization into irreducibles may not always be possible in general rings, since the procedure may continue indefinitely. However the procedure does stop for rings of integers. This comes from the fact that rings of integers are, again in modern terminology, what we call *noetherian rings*. The big picture can finally be summarized as follows:

- In general rings, factorization even into irreducibles may not be possible.
- In rings of integers, factorization into irreducibles is always possible, but may not be unique.
- For rings of integers which furthermore have a generalized Euclidean division, then the notions of prime and irreducible are equivalent, thus factorization is unique.

Let us now get back to the problem we are interested in, namely, factorization into product of irreducibles in rings of integers.

Example 2.1. Let $K = \mathbb{Q}(\sqrt{-5})$ be a quadratic number field, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, since $d \equiv 3 \pmod 4$. Let us prove that we do not have a unique factorization into product of irreducibles in $\mathbb{Z}[\sqrt{-5}]$. We have that

$$21 = 7 \cdot 3 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

with $3, 7, 1 \pm 2\sqrt{-5}$ irreducible. Let us show for example that 3 is irreducible. Let us write

$$3 = \alpha\beta,\ \alpha, \beta \in \mathcal{O}_K.$$

We need to see that either α or β is a unit (that is an invertible element of $\mathcal{O}_K$). The norm of 3 is given by

$$9 = \mathrm{N}_{K/\mathbb{Q}}(3) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathrm{N}_{K/\mathbb{Q}}(\beta),$$

by multiplicativity of the norm. By Corollary 1.10, we know that $N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$. Thus we get a factorization of 9 in $\mathbb{Z}$. There are only two possible factorizations over the integers:

- $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$, $\mathrm{N}_{K/\mathbb{Q}}(\beta) = \pm 9$ (or vice versa): by Corollary 1.11, we know that the element of $\mathcal{O}_K$ of norm ± 1 is a unit, and we are done.

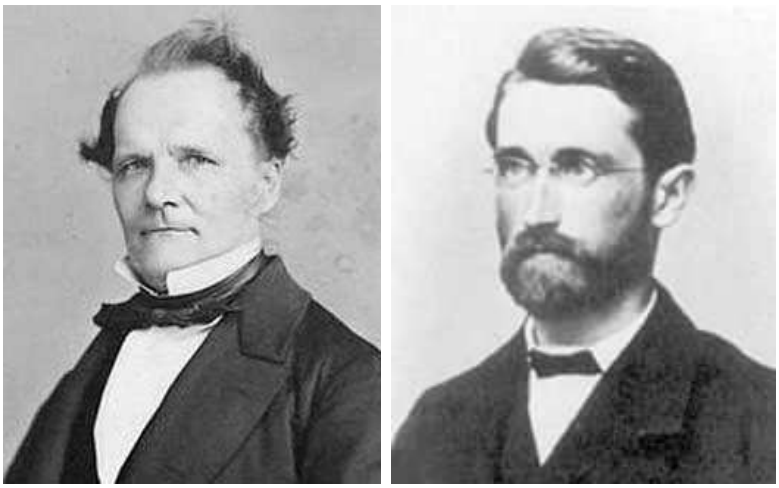


Figure 2.1: Ernst Kummer (1810-1893) and Richard Dedekind (1831-1916)

- $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 3$, $\mathrm{N}_{K/\mathbb{Q}}(\beta) = \pm 3$ (or vice versa): however, we will now show that there is no element of $\mathcal{O}_K$ with norm ± 3. Let us indeed assume that there exists $a + b\sqrt{-5} \in \mathcal{O}_K$, $a, b \in \mathbb{Z}$ such that

  $$\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = \pm 3.$$

  We can check that this equation has no solution modulo 5, yielding a contradiction.

On the other hand, we will see that the ideal $21\mathcal{O}_K$ can be factorized into 4 prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ such that

$$7\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,\ 3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_4,\ (1+2\sqrt{5})\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_3,\ (1-2\sqrt{5})\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_4,$$

namely

$$21\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

After the realization that uniqueness of factorization into irreducibles is unique in some rings of integers but not in others, the mathematician Kummer had the idea that one way to remedy to the situation could be to work with what he called *ideal numbers*, new structures which would enable us to regain the uniqueness of factorization. Ideals numbers then got called *ideals* by another mathematician, Dedekind, and this is the terminology that has remained. Ideals of $\mathcal{O}$ will the focus of this chapter.

Our goal will be to study ideals of $\mathcal{O}$, and in particular to show that we get a unique factorization into a product of prime ideals. To prove uniqueness, we need to study the arithmetic of non-zero ideals of $\mathcal{O}$, especially their behaviour under multiplication. We will recall how ideal multiplication is defined, which

will appear to be commutative and associative, with $\mathcal{O}$ itself as an identity. However, inverses need not exist, so we do not have a group structure. It turns out that we can get a group if we extend a bit the definition of ideals, which we will do by introducing *fractional ideals*, and showing that they are invertible.

2.2 Factorization and fractional ideals

Let us start by introducing the notion of norm of an ideal. We will see that in the case of principal ideals, we can relate the norm of the ideal with the norm of its generator.

Definition 2.1. Let I be a non-zero ideal of $\mathcal{O}$, we define the norm of I by

$$N(I) = |\mathcal{O}/I|.$$

Lemma 2.1. *Let I be a non-zero ideal of $\mathcal{O}$.*

1. *We have that*
$$N(\alpha\mathcal{O}) = |N_{K/\mathbb{Q}}(\alpha)|, \ \alpha \in \mathcal{O}.$$

2. *The norm of I is finite.*

Proof. 1. First let us notice that the formula we want to prove makes sense, since $N(\alpha) \in \mathbb{Z}$ when $\alpha \in \mathcal{O}_K$, thus $|N(\alpha)|$ is a positive integer. By Proposition 1.12, $\mathcal{O}$ is a free Abelian group of rank $n = [K : \mathbb{Q}]$, thus there exists a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}$, that is $\mathcal{O} = \mathbb{Z}\alpha_1 \oplus \cdots \mathbb{Z}\alpha_n$. It is now a general result on free Abelian groups that if H is as subgroup of G, both of same rank, with $\mathbb{Z}$-bases $x_1, \ldots, x_r$ and $y_1, \ldots, y_r$ respectively, with $y_i = \sum_j a_{ij}x_j$, then $|G/H| = |\det(a_{ij})|$. We thus apply this theorem in our case, where $G = \mathcal{O}$ and $H = \alpha\mathcal{O}$. Since one basis is obtained from the other by multiplication by α, we have that

$$|\mathcal{O}/\alpha\mathcal{O}| = |\det(\mu_\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|.$$

2. Let $0 \neq \alpha \in I$. Since I is an ideal of $\mathcal{O}$ and $\alpha\mathcal{O} \subset I$, we have a surjective map
$$\mathcal{O}/\alpha\mathcal{O} \to \mathcal{O}/I,$$
so that the result follows from part 1.

□

Example 2.2. Let $K = \mathbb{Q}(\sqrt{-17})$ be a quadratic number field, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$. Then

$$N(\langle 18\rangle) = 18^2.$$

Starting from now, we need to build up several intermediate results which we will use to prove the two most important results of this section. Let us begin with the fact that prime is a notion stronger than maximal. You may want to recall what is the general result for an arbitrary commutative ring and compare with respect to the case of a ring of integers (in general, maximal is stronger than prime).

Proposition 2.2. *Every non-zero prime ideal of $\mathcal{O}$ is maximal.*

Proof. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Since we have that

$$\mathfrak{p} \text{ is a maximal ideal of } \mathcal{O} \iff \mathcal{O}/\mathfrak{p} \text{ is a field},$$

it is enough to show that $\mathcal{O}/\mathfrak{p}$ is a field. In order to do so, let us consider $0 \neq x \in \mathcal{O}/\mathfrak{p}$, and show that x is invertible in $\mathcal{O}/\mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathcal{O}/\mathfrak{p}$ is an integral domain, thus the multiplication map $\mu_x : \mathcal{O}/\mathfrak{p} \mapsto \mathcal{O}/\mathfrak{p}$, $z \mapsto xz$, is injective (that is, its kernel is 0). By the above lemma, the cardinality of $\mathcal{O}/\mathfrak{p}$ is finite, thus μ_x being injective, it has to be also bijective. In other words μ_x is invertible, and there exists $y = \mu_x^{-1}(1) \in \mathcal{O}/\mathfrak{p}$. By definition, y is the inverse of x. □

To prove the next result, we need to first recall how to define the multiplication of two ideals.

Definition 2.2. If I and J are ideals of $\mathcal{O}$, we define the multiplication of ideals as follows:

$$IJ = \left\{ \sum_{finite} xy,\ x \in I,\ y \in J \right\}.$$

Example 2.3. Let $I = (\alpha_1, \alpha_2) = \alpha_1\mathcal{O} + \alpha_2\mathcal{O}$ and $J = (\beta_1, \beta_2) = \beta_1\mathcal{O} + \beta_2\mathcal{O}$, then

$$IJ = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2).$$

Lemma 2.3. *Let I be a non-zero ideal of $\mathcal{O}$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathcal{O}$ such that*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset I.$$

Proof. The idea of the proof goes as follows: we want to prove that every non-zero ideal I of $\mathcal{O}$ contains a product of r prime ideals. To prove it, we define a set $\mathcal{S}$ of all the ideals which do not contain a product of prime ideals, and we prove that this set is empty. To prove that this set is empty, we assume by contradiction that $\mathcal{S}$ does contain at least one non-zero ideal I. From this ideal, we will show that we can build another ideal I_1 such that I is strictly included in I_1, and by iteration we can build a sequence of ideals strictly included in each other, which will give a contradiction.

Let us now proceed. Let $\mathcal{S}$ be the set of all ideals which do not contain a product of prime ideals, and let I be in $\mathcal{S}$. First, note that I cannot be prime (otherwise I would contain a product of prime ideals with only one ideal, itself).

By definition of prime ideal, that means we can find $\alpha, \beta \in \mathcal{O}$ with $\alpha\beta \in I$, but $\alpha \notin I$, $\beta \notin I$. Using these two elements α and β, we can build two new ideals

$$J_1 = \alpha\mathcal{O} + I \supsetneq I, \;\; J_2 = \beta\mathcal{O} + I \supsetneq I,$$

with strict inclusion since $\alpha, \beta \notin I$.

To prove that J_1 or J_2 belongs to $\mathcal{S}$, we assume by contradiction that none are. Thus by definition of $\mathcal{S}$, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset J_1$ and $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset J_2$. Thus

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_r\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subset J_1J_2 \subset I$$

where the second inclusion holds since $\alpha\beta \in I$ and

$$J_1J_2 = (\alpha\mathcal{O} + I)(\beta\mathcal{O} + I) = \alpha\beta\mathcal{O} + \alpha I + \beta I + I^2 \in I$$

But $\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset I$ contradicts the fact that $I \in \mathcal{S}$. Thus J_1 or J_2 is in $\mathcal{S}$.

Starting from assuming that I is in $\mathcal{S}$, we have just shown that we can find another ideal, say I_1 (which is either J_1 or J_2), such that $I \subsetneq I_1$. Since I_1 is in $\mathcal{S}$ we can iterate the whole procedure, and find another ideal I_2 which strictly contains I_1, and so on and so forth. We thus get a strictly increasing sequence of ideals in $\mathcal{S}$:

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$$

Now by taking the norm of each ideal, we get a strictly decreasing sequence of integers

$$N(I) > N(I_1) > N(I_2) > \ldots,$$

which yields a contradiction and concludes the proof. □

Note that an ideal I of $\mathcal{O}$ is an $\mathcal{O}$-submodule of $\mathcal{O}$ with scalar multiplication given by $\mathcal{O} \times I \to I$, $(a, i) \mapsto ai$. Ideals of $\mathcal{O}$ are not invertible (with respect to ideal multiplication as defined above), so in order to get a group structure, we extend the definition and look at $\mathcal{O}$-submodules of K.

Definition 2.3. A fractional ideal I is a finitely generated $\mathcal{O}$-module contained in K.

Let $\alpha_1, \ldots, \alpha_r \in K$ be a set of generators for the fractional ideal I as $\mathcal{O}$-module. By Corollary 1.5, we can write $\alpha_i = \gamma_i/\delta_i$, $\gamma_i, \delta_i \in \mathcal{O}$ for $i = 1, \ldots, r$. Set

$$\delta = \prod_{i=1}^{r} \delta_i.$$

Since $\mathcal{O}$ is a ring, $\delta \in \mathcal{O}$. By construction, $J := \delta I$ is an ideal of $\mathcal{O}$. Thus for any fractional ideal $I \subset \mathcal{O}$, there exists an ideal $J \subset \mathcal{O}$ and $\delta \in \mathcal{O}$ such that

$$I = \frac{1}{\delta} J.$$

This yields an equivalent definition of fractional ideal.

Definition 2.4. An $\mathcal{O}$-submodule I of K is called a fractional ideal of $\mathcal{O}$ if there exists some non-zero $\delta \in \mathcal{O}$ such that $\delta I \subset \mathcal{O}$, that is $J = \delta I$ is an ideal of $\mathcal{O}$ and $I = \delta^{-1} J$.

It is easier to understand the terminology "fractional ideal" with the second definition.

Examples 2.4.
1. Ideals of $\mathcal{O}$ are particular cases of fractional ideals. They may be called integral ideals if there is an ambiguity.
2. The set
$$\frac{3}{2}\mathbb{Z} = \left\{ \frac{3x}{2} \in \mathbb{Q} \mid x \in \mathbb{Z} \right\}$$
is a fractional ideal.

It is now time to introduce the inverse of an ideal. We first do it in the particular case where the ideal is prime.

Lemma 2.4. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Define*
$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}\}.$$
1. *$\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$.*
2. *$\mathcal{O} \subsetneq \mathfrak{p}^{-1}$.*
3. *$\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$.*

Proof. 1. Let us start by showing that $\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$. Let $0 \neq a \in \mathfrak{p}$. By definition of $\mathfrak{p}^{-1}$, we have that $a\mathfrak{p}^{-1} \subset \mathcal{O}$. Thus $a\mathfrak{p}^{-1}$ is an integral ideal of $\mathcal{O}$, and $\mathfrak{p}^{-1}$ is a fractional ideal of $\mathcal{O}$.

2. We show that $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$. Clearly $\mathcal{O} \subset \mathfrak{p}^{-1}$. It is thus enough to find an element which is not an algebraic integer in $\mathfrak{p}^{-1}$. We start with any $0 \neq a \in \mathfrak{p}$. By Lemma 2.3, we choose the smallest r such that
$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)\mathcal{O}$$
for $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ prime ideals of $\mathcal{O}$. Since $(a)\mathcal{O} \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime, we have $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i by definition of prime. Without loss of generality, we can assume that $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Hence $\mathfrak{p}_1 = \mathfrak{p}$ since prime ideals in $\mathcal{O}$ are maximal (by Proposition 2.2). Furthermore, we have that
$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)\mathcal{O}$$
by minimality of r. Hence we can find $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ but not in $(a)\mathcal{O}$.

We are now ready to show that we have an element in $\mathfrak{p}^{-1}$ which is not in $\mathcal{O}$. This element is given by ba^{-1}.

- Using that $\mathfrak{p} = \mathfrak{p}_1$, we thus get $b\mathfrak{p} \subset (a)\mathcal{O}$, so $ba^{-1}\mathfrak{p} \subset \mathcal{O}$ and $ba^{-1} \in \mathfrak{p}^{-1}$.

- We also have $b \notin (a)\mathcal{O}$ and so $ba^{-1} \notin \mathcal{O}$.

This concludes the proof that $\mathfrak{p}^{-1} \neq \mathcal{O}$.

3. We now want to prove that $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. It is clear from the definition of $\mathfrak{p}^{-1}$ that $\mathfrak{p} = \mathfrak{p}\mathcal{O} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p} \subset \mathcal{O}$. Since $\mathfrak{p}$ is maximal (again by Proposition 2.2), $\mathfrak{p}\mathfrak{p}^{-1}$ is equal to $\mathfrak{p}$ or $\mathcal{O}$. It is now enough to prove that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ is not possible. Let us thus suppose by contradiction that $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Let $\{\beta_1, \ldots, \beta_r\}$ be a set of generators of $\mathfrak{p}$ as $\mathcal{O}$-module, and consider again $d := ab^{-1}$ which is in $\mathfrak{p}^{-1}$ but not in $\mathcal{O}$ (by the proof of 2.). Then we have that

$$d\beta_i \in \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p} \text{ and } d\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}.$$

Since $d\mathfrak{p} \subset \mathfrak{p}$, we have that

$$d\beta_i = \sum_{j=1}^{r} c_{ij}\beta_j \in \mathfrak{p},\ c_{ij} \in \mathcal{O},\ i = 1, \ldots, r,$$

or equivalently

$$0 = \sum_{j=1, j\neq i}^{r} c_{ij}\beta_j + \beta_i(c_{ii} - d),\ i = 1, \ldots, r.$$

The above r equations can be rewritten in a matrix equation as follows:

$$\underbrace{\begin{pmatrix} c_{11} - d & c_{1r} \\ c_{21} & c_{2r} \\ \vdots & \vdots \\ c_{r1} & c_{rr} - d \end{pmatrix}}_{C} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_r \end{pmatrix} = \mathbf{0}.$$

Thus the determinant of C is zero, while $\det(C)$ is an equation of degree r in d with coefficients in $\mathcal{O}$ of leading term ± 1. By Proposition 1.13, we have that d must be in $\mathcal{O}$, which is a contradiction.

□

Example 2.5. Consider the ideal $\mathfrak{p} = 3\mathbb{Z}$ of $\mathbb{Z}$. We have that

$$\mathfrak{p}^{-1} = \{x \in \mathbb{Q} \mid x \cdot 3\mathbb{Z} \subset \mathbb{Z}\} = \{x \in \mathbb{Q} \mid 3x \in \mathbb{Z}\} = \frac{1}{3}\mathbb{Z}.$$

We have

$$\mathfrak{p} \subset \mathbb{Z} \subset \mathfrak{p}^{-1} \subset \mathbb{Q}.$$

We can now prove that the fractional ideals of K form a group.

Theorem 2.5. *The non-zero fractional ideals of a number field K form a multiplicative group, denoted by I_K.*

Proof. The neutral element is $\mathcal{O}$. It is enough to show that every non-zero fractional ideal of $\mathcal{O}$ is invertible in I_K. By Lemma 2.4, we already know this is true for every prime (integral) ideals of $\mathcal{O}$.

Let us now show that this is true for every integral ideal of $\mathcal{O}$. Suppose by contradiction that there exists a non-invertible ideal I with its norm $N(I)$ minimal. Now I is included in a maximal integral $\mathfrak{p}$, which is also a prime ideal. Thus

$$I \subset \mathfrak{p}^{-1}I \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O},$$

where last equality holds by the above lemma. Let us show that $I \neq \mathfrak{p}^{-1}I$, so that the first inclusion is actually a strict inclusion. Suppose by contradiction that $I = \mathfrak{p}^{-1}I$. Let $d \in \mathfrak{p}^{-1}$ but not in $\mathcal{O}$ and let $\beta_1, \ldots, \beta_r$ be the set of generators of I as $\mathcal{O}$-module. We can thus write:

$$d\beta_i \in \mathfrak{p}^{-1}I = I,\ dI \subset \mathfrak{p}^{-1}I = I.$$

By the same argument as in the previous lemma, we get that d is in $\mathcal{O}$, a contradiction. We have thus found an ideal with $I \subsetneq \mathfrak{p}^{-1}I$, which implies that $N(I) > N(\mathfrak{p}^{-1}I)$. By minimality of $N(I)$, the ideal $\mathfrak{p}^{-1}I$ is invertible. Let $J \in I_K$ be its inverse, that is $J\mathfrak{p}^{-1}I = \mathcal{O}$. This shows that I is invertible, with inverse $J\mathfrak{p}^{-1}$.

If I is a fractional ideal, it can be written as $\frac{1}{d}J$ with J an integral ideal of $\mathcal{O}$ and $d \in \mathcal{O}$. Thus dJ^{-1} is the inverse of I. □

We can now prove unique factorization of integral ideals in $\mathcal{O} = \mathcal{O}_K$.

Theorem 2.6. *Every non-zero integral ideal I of $\mathcal{O}$ can be written in a unique way (up to permutation of the factors) as a product of prime ideals.*

Proof. We thus have to prove the existence of the factorization, and then the unicity up to permutation of the factors.

Existence. Let I be an integral ideal which does not admit such a factorization. We can assume that it is maximal among those ideals. Then I is not prime, but we will have $I \subset \mathfrak{p}$ for some maximal (hence prime) ideal. Thus $I\mathfrak{p}^{-1} \subset \mathcal{O}$ is an integral ideal and $I \subsetneq I\mathfrak{p}^{-1} \subset \mathcal{O}$, which strict inclusion, since if $I = I\mathfrak{p}^{-1}$, then it would imply that $\mathcal{O} = \mathfrak{p}^{-1}$. By maximality of I, the ideal $I\mathfrak{p}^{-1}$ must admit a factorization

$$I\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

that is

$$I = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

a contradiction.

Unicity. Let us assume that there exist two distinct factorizations of I, that is

$$I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

where $\mathfrak{p}_i$, $\mathfrak{q}_j$ are prime ideals, $i = 1, \ldots, r$, $j = 1, \ldots, s$. Let us assume by contradiction that $\mathfrak{p}_1$ is different from $\mathfrak{q}_j$ for all j. Thus we can choose $\alpha_j \in \mathfrak{q}_j$ but not in $\mathfrak{p}_1$, and we have that

$$\prod \alpha_j \in \prod \mathfrak{q}_j = I \subset \mathfrak{p}_1,$$

which contradicts the fact that $\mathfrak{p}_1$ is prime. Thus $\mathfrak{p}_1$ must be one of the $\mathfrak{q}_j$, say $\mathfrak{q}_1$. This gives that

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

We conclude by induction. □

Example 2.6. In $\mathbb{Q}(i)$, we have

$$(2)\mathbb{Z}[i] = (1+)^2\mathbb{Z}[i].$$

Corollary 2.7. *Let I be a non-zero fractional ideal. Then*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime integral ideals. This factorization is unique up to permutation of the factors.

Proof. A fractional ideal can be written as $d^{-1}I$, $d \in \mathcal{O}$, I an integral ideal. We write $I = \mathfrak{p}_1 \cdots \mathfrak{p}_t$ and $d\mathcal{O} = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Thus

$$(d\mathcal{O})^{-1}I = \mathfrak{p}_1 \cdots \mathfrak{p}_t \mathfrak{q}_q^{-1} \cdots \mathfrak{q}_n^{-1}.$$

It may be that some of the terms will cancel out, so that we end up with a factorization with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Unicity is proved as in the above theorem. □

2.3 The Chinese Theorem

We have defined in the previous section the group I_K of fractional ideals of a number field K, and we have proved that they have a unique factorization into a product of prime ideals. We are now interested in studying further properties of fractional ideals. The two main properties that we will prove are the fact that two elements are enough to generate these ideals, and that norms of ideals are multiplicative. Both properties can be proved as corollary of the Chinese theorem, that we first recall.

Theorem 2.8. *Let $I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$ be the factorization of an integral ideal I into a product of prime ideals $\mathfrak{p}_i$ with $\mathfrak{p}_i \neq \mathfrak{p}_j$ of $i \neq j$. Then there exists a canonical isomorphism*

$$\mathcal{O}/I \to \prod_{i=1}^m \mathcal{O}/\mathfrak{p}_i^{k_i}.$$

Corollary 2.9. *Let $I_1, \ldots, I_m$ be ideals which are pairwise coprime (that is $I_i + I_j = \mathcal{O}$ for $i \neq j$). Let $\alpha_1, \ldots, \alpha_m$ be elements of $\mathcal{O}$. Then there exists $\alpha \in \mathcal{O}$ with*

$$\alpha \equiv \alpha_i \mod I_i,\ i = 1, \ldots, m.$$

Proof. We can write $I_i = \prod \mathfrak{p}_{ij}^{n_{ij}}$. By hypothesis, no prime ideal occurs more than once as a $\mathfrak{p}_{ij}$, and each congruence is equivalent to the finite set of congruences

$$\alpha \equiv \alpha_i \mod \mathfrak{p}_{ij}^{n_{ij}},\ i, j.$$

Now write $I = \prod I_i$. Consider the vector $(\alpha_1, \ldots, \alpha_m)$ in $\prod_{i=1}^m \mathcal{O}/I_i$. The map

$$\mathcal{O}/I = \mathcal{O}/\prod I_i \to \prod_{i=1}^m \mathcal{O}/I_i$$

is surjective, thus there exists a preimage $\alpha \in \mathcal{O}$ of $(\alpha_1, \ldots, \alpha_m)$. □

Corollary 2.10. *Let I be a fractional ideal of $\mathcal{O}$, $\alpha \in I$. Then there exists $\beta \in I$ such that*

$$(\alpha, \beta) =< \alpha, \beta >= \alpha\mathcal{O} + \beta\mathcal{O} = I.$$

Proof. Let us first assume that I is an integral ideal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the prime factors of $\alpha\mathcal{O} \subset I$, so that I can be written as

$$I = \prod_{i=1}^m \mathfrak{p}_i^{k_i},\ k_i \geq 0.$$

Let us choose β_i in $\mathfrak{p}_i^{k_i}$ but not in $\mathfrak{p}_i^{k_i+1}$. By Corollary 2.9, there exists $\beta \in \mathcal{O}$ such that $\beta \equiv \beta_i \mod \mathfrak{p}_i^{k_i+1}$ for all $i = 1, \ldots, m$. Thus

$$\beta \in I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$$

and $\mathfrak{p}_i^{k_i}$ is the exact power of $\mathfrak{p}_i$ which divides $\beta\mathcal{O}$. In other words, $\beta\mathcal{O}I^{-1}$ is prime to $\alpha\mathcal{O}$, thus $\beta\mathcal{O}I^{-1} + \alpha\mathcal{O} = \mathcal{O}$, that is

$$\beta\mathcal{O} + \alpha I = I.$$

To conclude, we have that

$$I = \beta\mathcal{O} + \alpha I \subset \beta\mathcal{O} + \alpha\mathcal{O} \subset I.$$

If I is a fractional ideal, there exists by definition $d \in \mathcal{O}$ such that $I = \frac{1}{d}J$ with J an integral ideal. Thus $d\alpha \in J$. By the first part, there exists $\beta \in J$ such that $J = (d\alpha, \beta)$. Thus

$$I = \alpha\mathcal{O} + \frac{\beta}{d}\mathcal{O}.$$

□

We are now left to prove properties of the norm of an ideal, for which we need the following result.

Proposition 2.11. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ and $n > 0$. Then the $\mathcal{O}$-modules $\mathcal{O}/\mathfrak{p}$ and $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ are (non-canonically) isomorphic.*

Proof. We consider the map

$$\phi : \mathcal{O} \to \mathfrak{p}^n/\mathfrak{p}^{n+1},\ \alpha \mapsto \alpha\beta$$

for any β in $\mathfrak{p}^n$ but not in $\mathfrak{p}^{n+1}$. The proof consists of computing the kernel and the image of ϕ, and then of using one of the ring isomorphism theorems. This will conclude the proof since we will prove that $ker(\phi) = \mathfrak{p}$ and ϕ is surjective.

- Let us first compute the kernel of ϕ. If $\phi(\alpha) = 0$, then $\alpha\beta = 0$, which means that $\alpha\beta \in \mathfrak{p}^{n+1}$ that is $\alpha \in \mathfrak{p}$.

- Given any $\gamma \in \mathfrak{p}^n$, by Corollary 2.9, we can find $\gamma_1 \in \mathcal{O}$ such that

  $$\gamma_1 \equiv \gamma \mod \mathfrak{p}^{n+1},\ \gamma_1 \equiv 0 \mod \beta\mathcal{O}\mathfrak{p}^{-n},$$

  since $\beta\mathcal{O}\mathfrak{p}^{-n}$ is an ideal coprime to $\mathfrak{p}^{n+1}$. Since $\gamma \in \mathfrak{p}^n$, we have that γ_1 belongs to $\beta\mathcal{O}\mathfrak{p}^{-n} \cap \mathfrak{p}^n = \beta\mathcal{O}$ since $I \cap J = IJ$ when I and J are coprime ideals. In other words, $\gamma_1/\beta \in \mathcal{O}$. Its image by ϕ is

  $$\phi(\gamma_1/\beta) = (\gamma_1/\beta)\beta \mod \mathfrak{p}^{n+1} = \gamma.$$

  Thus ϕ is surjective.

□

Corollary 2.12. *Let I and J be two integral ideals. Then*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J).$$

Proof. Let us first assume that I and J are coprime. The chinese theorem tells us that

$$\mathcal{O}/IJ \simeq \mathcal{O}/I \times \mathcal{O}/J,$$

thus $|\mathcal{O}/IJ| = |\mathcal{O}/I||\mathcal{O}/J|$. We are left to prove that $\mathrm{N}(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p})^k$ for $k \geq 1$, $\mathfrak{p}$ a prime ideal. Now one of the isomorphism theorems for rings allows us to write that

$$\mathrm{N}(\mathfrak{p}^{k-1}) = |\mathcal{O}/\mathfrak{p}^{k-1}| = \left|\frac{\mathcal{O}/\mathfrak{p}^k}{\mathfrak{p}^{k-1}/\mathfrak{p}^k}\right| = \frac{|\mathcal{O}/\mathfrak{p}^k|}{|\mathfrak{p}^{k-1}/\mathfrak{p}^k|}.$$

By the above proposition, this can be rewritten as

$$\frac{|\mathcal{O}/\mathfrak{p}^k|}{|\mathcal{O}/\mathfrak{p}|} = \frac{\mathrm{N}(\mathfrak{p}^k)}{\mathrm{N}(\mathfrak{p})}.$$

Thus $\mathrm{N}(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p}^{k-1})\mathrm{N}(\mathfrak{p})$, and by induction on k, we conclude the proof. □

Example 2.7. In $\mathbb{Q}(i)$, we have that $(2)\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i]$ and thus

$$4 = N(2) = N(1+i)^2$$

and

$$N(1+i) = 2.$$

Definition 2.5. If $I = J_1 J_2^{-1}$ is a non-zero fractional ideal with J_1, J_2 integral ideals, we set

$$\mathrm{N}(I) = \frac{\mathrm{N}(J_1)}{\mathrm{N}(J_2)}.$$

This extends the norm N into a group homomorphism $\mathrm{N} : I_K \to \mathbb{Q}^\times$. For example, we have that $\mathrm{N}\left(\frac{2}{3}\mathbb{Z}\right) = \frac{2}{3}$.

The main definitions and results of this chapter are

- Definition of fractional ideals, the fact that they form a group I_K.
- Definition of norm of both integral and fractional ideals, and that the norm of ideals is multiplicative.
- The fact that ideals can be uniquely factorized into products of prime ideals.
- The fact that ideals can be generated with two elements: $I = (\alpha, \beta)$.

Chapter 3

Ramification Theory

This chapter introduces ramification theory, which roughly speaking asks the following question: if one takes a prime (ideal) $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of a number field K, what happens when $\mathfrak{p}$ is lifted to $\mathcal{O}_L$, that is $\mathfrak{p}\mathcal{O}_L$, where L is an extension of K. We know by the work done in the previous chapter that $\mathfrak{p}\mathcal{O}_L$ has a factorization as a product of primes, so the question is: will $\mathfrak{p}\mathcal{O}_L$ still be a prime? or will it factor somehow?

In order to study the behavior of primes in L/K, we first consider absolute extensions, that is when $K = \mathbb{Q}$, and define the notions of *discriminant*, *inertial degree* and *ramification index*. We show how the discriminant tells us about ramification. When we are lucky enough to get a "nice" ring of integers $\mathcal{O}_L$, that is $\mathcal{O}_L = \mathbb{Z}[\theta]$ for $\theta \in L$, we give a method to compute the factorization of primes in $\mathcal{O}_L$. We then generalize the concepts introduced to relative extensions, and study the particular case of Galois extensions.

3.1 Discriminant

Let K be a number field of degree n. Recall from Corollary 1.8 that there are n embeddings of K into $\mathbb{C}$.

Definition 3.1. Let K be a number field of degree n, and set

$$\begin{aligned} r_1 &= \text{number of real embeddings} \\ r_2 &= \text{number of pairs of complex embeddings} \end{aligned}$$

The couple (r_1, r_2) is called the signature of K. We have that

$$n = r_1 + 2r_2.$$

Examples 3.1.

1. The signature of $\mathbb{Q}$ is $(1, 0)$.
2. The signature of $\mathbb{Q}(\sqrt{d})$, $d > 0$, is $(2, 0)$.

3. The signature of $\mathbb{Q}(\sqrt{d})$, $d < 0$, is $(0, 1)$.

4. The signature of $\mathbb{Q}(\sqrt[3]{2})$ is $(1, 1)$.

Let K be a number field of degree n, and let $\mathcal{O}_K$ be its ring of integers. Let $\sigma_1, \ldots, \sigma_n$ be its n embeddings into $\mathbb{C}$. We define the map

$$\begin{aligned} \sigma \quad : K &\to \quad \mathbb{C}^n \\ x &\mapsto \quad (\sigma_1(x), \ldots, \sigma_n(x)). \end{aligned}$$

Since $\mathcal{O}_K$ is a free abelian group of rank n, we have a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathcal{O}_K$. Let us consider the $n \times n$ matrix M given by

$$M = (\sigma_i(\alpha_j))_{1 \leq i,j \leq n}.$$

The determinant of M is a measure of the density of $\mathcal{O}_K$ in K (actually of $K/\mathcal{O}_K$). It tells us how sparse the integers of K are. However, $\det(M)$ is only defined up to sign, and is not necessarily in either $\mathbb{R}$ or K. So instead we consider

$$\begin{aligned} \det(M^2) &= \det(M^t M) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right)_{i,j} \\ &= \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j} \in \mathbb{Z}, \end{aligned}$$

and this does not depend on the choice of a basis.

Definition 3.2. Let $\alpha_1, \ldots, \alpha_n \in K$. We define

$$disc(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j}.$$

In particular, if $\alpha_1, \ldots, \alpha_n$ is any $\mathbb{Z}$-basis of $\mathcal{O}_K$, we write Δ_K, and we call discriminant the integer

$$\Delta_K = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{1 \leq i,j \leq n}.$$

We have that $\Delta_K \neq 0$. This is a consequence of the following lemma.

Lemma 3.1. *The symmetric bilinear form*

$$\begin{aligned} K \times K &\to \mathbb{Q} \\ (x, y) &\mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy) \end{aligned}$$

is non-degenerate.

Proof. Let us assume by contradiction that there exists $0 \neq \alpha \in K$ such that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = 0$ for all $\beta \in K$. By taking $\beta = \alpha^{-1}$, we get

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = n \neq 0.$$

□

Now if we had that $\Delta_K = 0$, there would be a non-zero column vector $(x_1, \ldots, x_n)^t$, $x_i \in \mathbb{Q}$, killed by the matrix $(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{1\leq i,j\leq n}$. Set $\gamma = \sum_{i=1}^n \alpha_i x_i$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_j\gamma) = 0$ for each j, which is a contradiction by the above lemma.

Example 3.2. Consider the quadratic field $K = \mathbb{Q}(\sqrt{5})$. Its two embeddings into $\mathbb{C}$ are given by

$$\sigma_1 : a + b\sqrt{5} \mapsto a + b\sqrt{5},\ \sigma_2 : a + b\sqrt{5} \mapsto a - b\sqrt{5}.$$

Its ring of integers is $\mathbb{Z}[(1+\sqrt{5})/2]$, so that the matrix M of embeddings is

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}$$

and its discriminant Δ_K can be computed by

$$\Delta_K = \det(M^2) = 5.$$

3.2 Prime decomposition

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Indeed, one easily verifies that this is an ideal of $\mathbb{Z}$. Now if a, b are integers with $ab \in \mathfrak{p} \cap \mathbb{Z}$, then we can use the fact that $\mathfrak{p}$ is prime to deduce that either a or b belongs to $\mathfrak{p}$ and thus to $\mathfrak{p} \cap \mathbb{Z}$ (note that $\mathfrak{p} \cap \mathbb{Z}$ is a proper ideal since $\mathfrak{p} \cap \mathbb{Z}$ does not contain 1, and $\mathfrak{p} \cap \mathbb{Z} \neq \emptyset$, as $\mathrm{N}(\mathfrak{p})$ belongs to $\mathfrak{p}$ and $\mathbb{Z}$ since $\mathrm{N}(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| < \infty$).

Since $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, there must exist a prime number p such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We say that $\mathfrak{p}$ is above p.

$$\begin{array}{c} \mathfrak{p} \subset \mathcal{O}_K \subset K \\ \Big| \\ p\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \end{array}$$

We call residue field the quotient of a commutative ring by a maximal ideal. Thus the residue field of $p\mathbb{Z}$ is $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. We are now interested in the residue field $\mathcal{O}_K/\mathfrak{p}$. We show that $\mathcal{O}_K/\mathfrak{p}$ is a $\mathbb{F}_p$-vector space of finite dimension. Set

$$\phi : \mathbb{Z} \to \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p},$$

where the first arrow is the canonical inclusion ι of $\mathbb{Z}$ into $\mathcal{O}_K$, and the second arrow is the projection π, so that $\phi = \pi \circ \iota$. Now the kernel of ϕ is given by

$$ker(\phi) = \{a \in \mathbb{Z} \mid a \in \mathfrak{p}\} = \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z},$$

so that ϕ induces an injection of $\mathbb{Z}/p\mathbb{Z}$ into $\mathcal{O}_K/\mathfrak{p}$, since $\mathbb{Z}/p\mathbb{Z} \simeq Im(\phi) \subset \mathcal{O}_K/\mathfrak{p}$. By Lemma 2.1, $\mathcal{O}_K/\mathfrak{p}$ is a finite set, thus a finite field which contains $\mathbb{Z}/p\mathbb{Z}$ and we have indeed a finite extension of $\mathbb{F}_p$.

Definition 3.3. We call inertial degree, and we denote by $f_{\mathfrak{p}}$, the dimension of the $\mathbb{F}_p$-vector space $\mathcal{O}/\mathfrak{p}$, that is

$$f_{\mathfrak{p}} = \dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p}).$$

Note that we have

$$\mathrm{N}(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| = |\mathbb{F}_p^{\dim_{\mathbb{F}_p}(\mathcal{O}/\mathfrak{p})}| = |\mathbb{F}_p|^{f_{\mathfrak{p}}} = p^{f_{\mathfrak{p}}}.$$

Example 3.3. Consider the quadratic field $K = \mathbb{Q}(i)$, with ring of integers $\mathbb{Z}[i]$, and let us look at the ideal $2\mathbb{Z}[i]$:

$$2\mathbb{Z}[i] = (1+i)(1-i)\mathbb{Z}[i] = \mathfrak{p}^2,\ \mathfrak{p} = (1+i)\mathbb{Z}[i]$$

since $(-i)(1+i) = 1-i$. Furthermore, $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$, so that $\mathfrak{p} = (1+i)$ is said to be above 2. We have that

$$\mathrm{N}(\mathfrak{p}) = N_{K/\mathbb{Q}}(1+i) = (1+i)(1-i) = 2$$

and thus $f_{\mathfrak{p}} = 1$. Indeed, the corresponding residue field is

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_2.$$

Let us consider again a prime ideal $\mathfrak{p}$ of $\mathcal{O}$. We have seen that $\mathfrak{p}$ is above the ideal $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. We can now look the other way round: we start with the prime $p \in \mathbb{Z}$, and look at the ideal $p\mathcal{O}$ of $\mathcal{O}$. We know that $p\mathcal{O}$ has a unique factorization into a product of prime ideals (by all the work done in Chapter 2). Furthermore, we have that $p \subset \mathfrak{p}$, thus $\mathfrak{p}$ has to be one of the factors of $p\mathcal{O}$.

Definition 3.4. Let $p \in \mathbb{Z}$ be a prime. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ above p. We call ramification index of $\mathfrak{p}$, and we write $e_{\mathfrak{p}}$, the exact power of $\mathfrak{p}$ which divides $p\mathcal{O}$.

We start from $p \in \mathbb{Z}$, whose factorization in $\mathcal{O}$ is given by

$$p\mathcal{O} = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_g^{e_{\mathfrak{p}_g}}.$$

We say that p is ramified if $e_{\mathfrak{p}_i} > 1$ for some i. On the contrary, p is non-ramified if

$$p\mathcal{O} = \mathfrak{p}_1 \cdots \mathfrak{p}_g,\ \mathfrak{p}_i \neq \mathfrak{p}_j,\ i \neq j.$$

Both the inertial degree and the ramification index are connected via the degree of the number field as follows.

Proposition 3.2. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $p \in \mathbb{Z}$ and let*

$$p\mathcal{O} = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_g^{e_{\mathfrak{p}_g}}$$

be its factorization in $\mathcal{O}$. We have that

$$n = [K : \mathbb{Q}] = \sum_{i=1}^{g} e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}.$$

Proof. By Lemma 2.1, we have

$$\mathrm{N}(p\mathcal{O}) = |\mathrm{N}_{K/\mathbb{Q}}(p)| = p^n,$$

where $n = [K : \mathbb{Q}]$. Since the norm N is multiplicative (see Corollary 2.12), we deduce that

$$\mathrm{N}(\mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_g^{e_{\mathfrak{p}_g}}) = \prod_{i=1}^{g} \mathrm{N}(\mathfrak{p}_i)^{e_{\mathfrak{p}_i}} = \prod_{i=1}^{g} p^{f_{\mathfrak{p}_i} e_{\mathfrak{p}_i}}.$$

□

There is, in general, no straightforward method to compute the factorization of $p\mathcal{O}$. However, in the case where the ring of integers $\mathcal{O}$ is of the form $\mathcal{O} = \mathbb{Z}[\theta]$, we can use the following result.

Proposition 3.3. *Let K be a number field, with ring of integers $\mathcal{O}_K$, and let p be a prime. Let us assume that there exists θ such that $\mathcal{O} = \mathbb{Z}[\theta]$, and let f be the minimal polynomial of θ, whose reduction modulo p is denoted by $\bar{f}$. Let*

$$\bar{f}(X) = \prod_{i=1}^{g} \phi_i(X)^{e_i}$$

be the factorization of $f(X)$ in $\mathbb{F}_p[X]$, with $\phi_i(X)$ coprime and irreducible. We set

$$\mathfrak{p}_i = (p, f_i(\theta)) = p\mathcal{O} + f_i(\theta)\mathcal{O}$$

where f_i is any lift of ϕ_i to $\mathbb{Z}[X]$, that is $\bar{f}_i = \phi_i \mod p$. Then

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

is the factorization of $p\mathcal{O}$ in $\mathcal{O}$.

Proof. Let us first notice that we have the following isomorphism

$$\mathcal{O}/p\mathcal{O} = \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \simeq \frac{\mathbb{Z}[X]/f(X)}{p(\mathbb{Z}[X]/f(X))} \simeq \mathbb{Z}[X]/(p, f(X)) \simeq \mathbb{F}_p[X]/\bar{f}(X),$$

where $\bar{f}$ denotes $f \mod p$. Let us call A the ring

$$A = \mathbb{F}_p[X]/\bar{f}(X).$$

The inverse of the above isomorphism is given by the evaluation in θ, namely, if $\psi(X) \in \mathbb{F}_p[X]$, with $\psi(X) \mod \bar{f}(X) \in A$, and $g \in \mathbb{Z}[X]$ such that $\bar{g} = \psi$, then its preimage is given by $g(\theta)$. By the Chinese Theorem, recall that we have

$$A = \mathbb{F}_p[X]/\bar{f}(X) \simeq \prod_{i=1}^{g} \mathbb{F}_p[X]/\phi_i(X)^{e_i},$$

since by assumption, the ideal $(\bar{f}(X))$ has a prime factorization given by $(\bar{f}(X)) = \prod_{i=1}^{g} (\phi_i(X))^{e_i}$.

We are now ready to understand the structure of prime ideals of both $\mathcal{O}/p\mathcal{O}$ and A, thanks to which we will prove that $\mathfrak{p}_i$ as defined in the assumption is prime, that any prime divisor of $p\mathcal{O}$ is actually one of the $\mathfrak{p}_i$, and that the power e_i appearing in the factorization of $\bar{f}$ are bigger or equal to the ramification index $e_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$. We will then invoke the proposition that we have just proved to show that $e_i = e_{\mathfrak{p}_i}$, which will conclude the proof.

By the factorization of A given above by the Chinese theorem, the maximal ideals of A are given by $(\phi_i(X))A$, and the degree of the extension $A/(\phi_i(X))A$ over $\mathbb{F}_p$ is the degree of ϕ_i. By the isomorphism $A \simeq \mathcal{O}/p\mathcal{O}$, we get similarly that the maximal ideals of $\mathcal{O}/p\mathcal{O}$ are the ideals generated by $f_i(\theta) \mod p\mathcal{O}$.

We consider the projection $\pi : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$. We have that

$$\pi(\mathfrak{p}_i) = \pi(p\mathcal{O} + f_i(\theta)\mathcal{O}) = f_i(\theta)\mathcal{O} \mod p\mathcal{O}.$$

Consequently, $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}$, since $f_i(\theta)\mathcal{O}$ is. Furthermore, since $\mathfrak{p}_i \supset p\mathcal{O}$, we have $\mathfrak{p}_i \mid p\mathcal{O}$, and the inertial degree $f_{\mathfrak{p}_i} = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$ is the degree of ϕ_i, while $e_{\mathfrak{p}_i}$ denotes the ramification index of $\mathfrak{p}_i$.

Now, every prime ideal $\mathfrak{p}$ in the factorization of $p\mathcal{O}$ is one of the $\mathfrak{p}_i$, since the image of $\mathfrak{p}$ by π is a maximal ideal of $\mathcal{O}/p\mathcal{O}$, that is

$$p\mathcal{O} = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_g^{e_{\mathfrak{p}_g}}$$

and we are thus left to look at the ramification index.

The ideal $\phi_i^{e_i} A$ of A belongs to $\mathcal{O}/p\mathcal{O}$ via the isomorphism between $\mathcal{O}/p\mathcal{O} \simeq A$, and its preimage in $\mathcal{O}$ by π^{-1} contains $\mathfrak{p}_i^{e_i}$ (since if $\alpha \in \mathfrak{p}_i^{e_i}$, then α is a sum of products $\alpha_1 \cdots \alpha_{e_i}$, whose image by π will be a sum of product $\pi(\alpha_1) \cdots \pi(\alpha_{e_i})$ with $\pi(\alpha_i) \in \phi_i A$). In $\mathcal{O}/p\mathcal{O}$, we have $0 = \cap_{i=1}^g \phi_i(\theta)^{e_i}$, that is

$$p\mathcal{O} = \pi^{-1}(0) = \cap_{i=1}^g \pi^{-1}(\phi_i^{e_i} A) \supset \cap_{i=1}^g \mathfrak{p}_i^{e_i} = \prod_{i=1}^g \mathfrak{p}_i^{e_i}.$$

We then have that this last product is divided by $p\mathcal{O} = \prod \mathfrak{p}_i^{e_{\mathfrak{p}_i}}$, that is $e_i \geq e_{\mathfrak{p}_i}$.

Let $n = [K : \mathbb{Q}]$. To show that we have equality, that is $e_i = e_{\mathfrak{p}_i}$, we use the previous proposition:

$$n = [K : \mathbb{Q}] = \sum_{i=1}^g e_{\mathfrak{p}_i} f_{\mathfrak{p}_i} \leq \sum_{i=1}^g e_i \deg(\phi_i) = \dim_{\mathbb{F}_p}(A) = \dim_{\mathbb{F}_p} \mathbb{Z}^n/p\mathbb{Z}^n = n.$$

□

The above proposition gives a concrete method to compute the factorization of a prime $p\mathcal{O}_K$:

1. Choose a prime $p \in \mathbb{Z}$ whose factorization in $p\mathcal{O}_K$ is to be computed.

2. Let f be the minimal polynomial of θ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

3. Compute the factorization of $\bar{f} = f \mod p$:

$$\bar{f} = \prod_{i=1}^{g} \phi_i(X)^{e_i}.$$

4. Lift each ϕ_i in a polynomial $f_i \in \mathbb{Z}[X]$.

5. Compute $\mathfrak{p}_i = (p, f_i(\theta))$ by evaluating f_i in θ.

6. The factorization of $p\mathcal{O}$ is given by

$$p\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

Examples 3.4. 1. Let us consider $K = \mathbb{Q}(\sqrt[3]{2})$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. We want to factorize $5\mathcal{O}_K$. By the above proposition, we compute

$$\begin{aligned} X^3 - 2 &\equiv (X-3)(X^2+3X+4) \\ &\equiv (X+2)(X^2-2X-1) \mod 5. \end{aligned}$$

We thus get that

$$5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,\ \mathfrak{p}_1 = (5, 2+\sqrt[3]{2}),\ \mathfrak{p}_2 = (5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1).$$

2. Let us consider $\mathbb{Q}(i)$, with $\mathcal{O}_K = \mathbb{Z}[i]$, and choose $p = 2$. We have $\theta = i$ and $f(X) = X^2 + 1$. We compute the factorization of $\bar{f}(X) = f(X) \mod 2$:

$$X^2 + 1 \equiv X^2 - 1 \equiv (X-1)(X+1) \equiv (X-1)^2 \mod 2.$$

We can take any lift of the factors to $\mathbb{Z}[X]$, so we can write

$$2\mathcal{O}_K = (2, i-1)(2, i+1) \text{ or } 2 = (2, i-1)^2$$

which is the same, since $(2, i-1) = (2, 1+i)$. Furthermore, since $2 = (1-i)(1+i)$, we see that $(2, i-1) = (1+i)$, and we recover the result of Example 3.3.

Definition 3.5. We say that p is inert if $p\mathcal{O}$ is prime, in which case we have $g = 1$, $e = 1$ and $f = n$. We say that p is totally ramified if $e = n$, $g = 1$, and $f = 1$.

The discriminant of K gives us information on the ramification in K.

Theorem 3.4. *Let K be a number field. If p is ramified, then p divides the discriminant Δ_K.*

Proof. Let $\mathfrak{p} \mid p\mathcal{O}$ be an ideal such that $\mathfrak{p}^2 \mid p\mathcal{O}$ (we are just rephrasing the fact that p is ramified). We can write $p\mathcal{O} = \mathfrak{p}I$ with I divisible by all the primes above p ($\mathfrak{p}$ is voluntarily left as a factor of I). Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$ be a $\mathbb{Z}$-basis of $\mathcal{O}$ and let $\alpha \in I$ but $\alpha \notin p\mathcal{O}$. We write

$$\alpha = b_1\alpha_1 + \ldots + b_n\alpha_n,\ b_i \in \mathbb{Z}.$$

Since $\alpha \notin p\mathcal{O}$, there exists a b_i which is not divisible by p, say b_1. Recall that

$$\Delta_K = \det \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

where σ_i, $i = 1, \ldots, n$ are the n embeddings of K into $\mathbb{C}$. Let us replace α_1 by α, and set

$$D = \det \begin{pmatrix} \sigma_1(\alpha) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2.$$

Now D and Δ_K are related by

$$D = \Delta_K b_1^2,$$

since D can be rewritten as

$$D = \det \left(\begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ b_2 & 1 & & 0 \\ & & \ddots & \\ b_n & & \ldots & 1 \end{pmatrix} \right)^2.$$

We are thus left to prove that $p \mid D$, since by construction, we have that p does not divide b_1^2.

Intuitively, the trick of this proof is to replace proving that $p|\Delta_K$ where we have no clue how the factor p appears, with proving that $p|D$, where D has been built on purpose as a function of a suitable α which we will prove below is such that all its conjugates are above p.

Let L be the Galois closure of K, that is, L is a field which contains K, and which is a normal extension of $\mathbb{Q}$. The conjugates of α all belong to L. We know that α belongs to all the primes of $\mathcal{O}_K$ above p. Similarly, $\alpha \in K \subset L$ belongs to all primes $\mathfrak{P}$ of $\mathcal{O}_L$ above p. Indeed, $\mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ above p, which contains α.

We now fix a prime $\mathfrak{P}$ above p in $\mathcal{O}_L$. Then $\sigma_i(\mathfrak{P})$ is also a prime ideal of $\mathcal{O}_L$ above p ($\sigma_i(\mathfrak{P})$ is in L since $L/\mathbb{Q}$ is Galois, $\sigma_i(\mathfrak{P})$ is prime since $\mathfrak{P}$ is, and $p = \sigma_i(p) \in \sigma_i(\mathfrak{P})$). We have that $\sigma_i(\alpha) \in \mathfrak{P}$ for all σ_i, thus the first column of the matrix involves in the computation of D is in $\mathfrak{P}$, so that $D \in \mathfrak{P}$ and $D \in \mathbb{Z}$, to get

$$D \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}.$$

□

We have just proved that if p is ramified, then $p|\Delta_K$. The converse is also true.

Examples 3.5. 1. We have seen in Example 3.2 that the discriminant of $K = \mathbb{Q}(\sqrt{5})$ is $\Delta_K = 5$. This tells us that only 5 is ramified in $\mathbb{Q}(\sqrt{5})$.

2. In Example 3.3, we have seen that 2 ramifies in $K = \mathbb{Q}(i)$. So 2 should appear in Δ_K. One can actually check that $\Delta_K = -4$.

Corollary 3.5. *There is only a finite number of ramified primes.*

Proof. The discriminant only has a finite number of divisors. □

3.3 Relative Extensions

Most of the theory seen so far assumed that the base field is $\mathbb{Q}$. In most cases, this can be generalized to an arbitrary number field K, in which case we consider a number field extension L/K. This is called a relative extension. By contrast, we may call absolute an extension whose base field is $\mathbb{Q}$. Below, we will generalize several definitions previously given for absolute extensions to relative extensions.

Let K be a number field, and let L/K be a finite extension. We have correspondingly a ring extension $\mathcal{O}_K \to \mathcal{O}_L$. If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$, then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. We say that $\mathfrak{P}$ is above $\mathfrak{p}$. We have a factorization

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}},$$

where $e_{\mathfrak{P}_i/\mathfrak{p}}$ is the relative ramification index. The relative inertial degree is given by

$$f_{\mathfrak{P}_i|\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

We still have that

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

where the summation is over all $\mathfrak{P}$ above $\mathfrak{p}$.

Let $M/L/K$ be a tower of finite extensions, and let $\mathcal{P}, \mathfrak{P}, \mathfrak{p}$ be prime ideals of respectively M, L, and K. Then we have that

$$\begin{aligned} f_{\mathcal{P}|\mathfrak{p}} &= f_{\mathcal{P}|\mathfrak{P}} f_{\mathfrak{P}|\mathfrak{p}} \\ e_{\mathcal{P}|\mathfrak{p}} &= e_{\mathcal{P}|\mathfrak{P}} e_{\mathfrak{P}|\mathfrak{p}}. \end{aligned}$$

Let I_K, I_L be the groups of fractional ideals of K and L respectively. We can also generalize the application norm as follows:

$$\begin{aligned} \mathrm{N} : \quad I_L &\to I_K \\ \mathfrak{P} &\mapsto \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}}, \end{aligned}$$

which is a group homomorphism. This defines a relative norm for ideals, which is itself an ideal!

In order to generalize the discriminant, we would like to have an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ (similarly to having a $\mathbb{Z}$-basis of $\mathcal{O}_K$), however such a basis does not exist in general. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L where $\alpha_i \in \mathcal{O}_L$, $i = 1, \ldots, n$. We set

$$disc_{L/K}(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

where $\sigma_i : L \to \mathbb{C}$ are the embeddings of L into $\mathbb{C}$ which fix K. We define $\Delta_{L/K}$ as the ideal generated by all $disc_{L/K}(\alpha_1, \ldots, \alpha_n)$. It is called relative discriminant.

3.4 Normal Extensions

Let L/K be a Galois extension of number fields, with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. If $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in $\mathcal{O}_L$, and $\sigma \in G$, then $\sigma(\mathfrak{P})$ is a prime ideal above $\mathfrak{p}$. Indeed, $\sigma(\mathfrak{P}) \cap \mathcal{O}_K \subset K$, thus $\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \mathfrak{P} \cap \mathcal{O}_K$ since K is fixed by σ.

Theorem 3.6. *Let*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

be the factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$. Then G acts transitively on the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$. Furthermore, we have that

$$e_1 = \ldots = e_g = e \text{ where } e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$$
$$f_1 = \ldots = f_g = f \text{ where } f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$$

and

$$[L : K] = efg.$$

Proof. G **acts transitively.** Let $\mathfrak{P}$ be one of the $\mathfrak{P}_i$. We need to prove that there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_j) = \mathfrak{P}$ for $\mathfrak{P}_j$ any other of the $\mathfrak{P}_i$. In the proof of Corollary 2.10, we have seen that there exists $\beta \in \mathfrak{P}$ such that $\beta\mathcal{O}_L\mathfrak{P}^{-1}$ is an integral ideal coprime to $\mathfrak{p}\mathcal{O}_L$. The ideal

$$I = \prod_{\sigma \in G} \sigma(\beta\mathcal{O}_L\mathfrak{P}^{-1})$$

is an integral ideal of $\mathcal{O}_L$ (since $\beta\mathcal{O}_L\mathfrak{P}^{-1}$ is), which is furthermore coprime to $\mathfrak{p}\mathcal{O}_L$ (since $\sigma(\beta\mathcal{O}_L\mathfrak{P}^{-1})$ and $\sigma(\mathfrak{p}\mathcal{O}_L)$ are coprime and $\sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{p})\sigma(\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$).

Thus I can be rewritten as

$$\begin{aligned} I &= \frac{\prod_{\sigma\in G}\sigma(\beta)\mathcal{O}_L}{\prod_{\sigma\in G}\sigma(\mathfrak{P})} \\ &= \frac{N_{L/K}(\beta)\mathcal{O}_L}{\prod_{\sigma\in G}\sigma(\mathfrak{P})} \end{aligned}$$

and we have that

$$I\prod_{\sigma\in G}\sigma(\mathfrak{P}) = N_{L/K}(\beta)\mathcal{O}_L.$$

Since $N_{L/K}(\beta) = \prod_{\sigma\in G}\sigma(\beta)$, $\beta\in\mathfrak{P}$ and one of the σ is the identity, we have that $N_{L/K}(\beta)\in\mathfrak{P}$. Furthermore, $N_{L/K}(\beta)\in\mathcal{O}_K$ since $\beta\in\mathcal{O}_L$, and we get that $N_{L/K}(\beta)\in\mathfrak{P}\cap\mathcal{O}_K = \mathfrak{p}$, from which we deduce that $\mathfrak{p}$ divides the right hand side of the above equation, and thus the left hand side. Since I is coprime to $\mathfrak{p}$, we get that $\mathfrak{p}$ divides $\prod_{\sigma\in G}\sigma(\mathfrak{P})$. In other words, using the factorization of $\mathfrak{p}$, we have that

$$\prod_{\sigma\in G}\sigma(\mathfrak{P}) \text{ is divisible by } \mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g}\mathfrak{P}_i^{e_i}$$

and each of the $\mathfrak{P}_i$ has to be among $\{\sigma(\mathfrak{P})\}_{\sigma\in G}$.

All the ramification indices are equal. By the first part, we know that there exists $\sigma\in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_k$, $i\neq k$. Now, we have that

$$\begin{aligned} \sigma(\mathfrak{p}\mathcal{O}_L) &= \prod_{i=1}^{g}\sigma(\mathfrak{P}_i)^{e_i} \\ &= \mathfrak{p}\mathcal{O}_L \\ &= \prod_{i=1}^{g}\mathfrak{P}_i^{e_i} \end{aligned}$$

where the second equality holds since $\mathfrak{p}\in\mathcal{O}_K$ and L/K is Galois. By comparing the two factorizations of $\mathfrak{p}$ and its conjugates, we get that $e_i = e_k$.

All the inertial degrees are equal. This follows from the fact that σ induces the following field isomorphism

$$\mathcal{O}_L/\mathfrak{P}_i \simeq \mathcal{O}_L/\sigma(\mathfrak{P}_i).$$

Finally we have that

$$|G| = [L:K] = efg.$$

□

For now on, let us fix $\mathfrak{P}$ above $\mathfrak{p}$.

Definition 3.6. The stabilizer of $\mathfrak{P}$ in G is called the decomposition group, given by

$$D = D_{\mathfrak{P}/\mathfrak{p}} = \{\sigma\in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} < G.$$

The index $[G : D]$ must be equal to the number of elements in the orbit $G\mathfrak{P}$ of $\mathfrak{P}$ under the action of G, that is $[G : D] = |G\mathfrak{P}|$ (this is the orbit-stabilizer theorem).

By the above theorem, we thus have that $[G : D] = g$, where g is the number of distinct primes which divide $\mathfrak{p}\mathcal{O}_L$. Thus

$$\begin{aligned} n &= efg \\ &= ef\frac{|G|}{|D|} \end{aligned}$$

and

$$|D| = ef.$$

If $\mathfrak{P}'$ is another prime ideal above $\mathfrak{p}$, then the decomposition groups $D_{\mathfrak{P}/\mathfrak{p}}$ and $D_{\mathfrak{P}'/\mathfrak{p}}$ are conjugate in G via any Galois automorphism mapping $\mathfrak{P}$ to $\mathfrak{P}'$ (in formula, we have that if $\mathfrak{P}' = \tau(\mathfrak{P})$, then $\tau D_{\mathfrak{P}/\mathfrak{p}}\tau^{-1} = D_{\tau(\mathfrak{P})/\mathfrak{p}}$).

Proposition 3.7. *Let $D = D_{\mathfrak{P}/\mathfrak{p}}$ be the decomposition group of $\mathfrak{P}$. The subfield*

$$L^D = \{\alpha \in L \mid \sigma(\alpha) = \alpha,\ \sigma \in D\}$$

is the smallest subfield M of L such that $(\mathfrak{P} \cap \mathcal{O}_M)\mathcal{O}_L$ does not split. It is called the decomposition field of $\mathfrak{P}$.

Proof. We first prove that L/L^D has the property that$(\mathfrak{P} \cap \mathcal{O}_{L^D})\mathcal{O}_L$ does not split. We then prove its minimality.

We know by Galois theory that $\mathrm{Gal}(L/L^D)$ is given by D. Furthermore, the extension L/L^D is Galois since L/K is. Let $\mathfrak{Q} = \mathfrak{P} \cap \mathcal{O}_{L^D}$ be a prime below $\mathfrak{P}$. By Theorem 3.6, we know that D acts transitively on the set of primes above $\mathfrak{Q}$, among which is $\mathfrak{P}$. Now by definition of $D = D_{\mathfrak{P}/\mathfrak{p}}$, we know that $\mathfrak{P}$ is fixed by D. Thus there is only $\mathfrak{P}$ above $\mathfrak{Q}$.

Let us now prove the minimality of L^D. Assume that there exists a field M with $L/M/K$, such that $\mathfrak{Q} = \mathfrak{P} \cap \mathcal{O}_M$ has only one prime ideal of $\mathcal{O}_L$ above it. Then this unique ideal must be $\mathfrak{P}$, since by definition $\mathfrak{P}$ is above $\mathfrak{Q}$. Then $\mathrm{Gal}(L/M)$ is a subgroup of D, since its elements are fixing $\mathfrak{P}$. Thus $M \supset L^D$. □

$$\begin{array}{c} L \supset \mathfrak{P} \\ {\scriptstyle \frac{n}{g}}\Big| D \\ L^D \supset \mathfrak{Q} \\ {\scriptstyle g}\Big| G/D \\ K \supset \mathfrak{p} \end{array}$$

terminology	e	f	g
inert	1	n	1
totally ramified	n	1	1
(totally) split	1	1	n

Table 3.1: Different prime behaviors

The next proposition uses the same notation as the above proof.

Proposition 3.8. *Let $\mathfrak{Q}$ be the prime of L^D below $\mathfrak{P}$. We have that*

$$f_{\mathfrak{Q}/\mathfrak{p}} = e_{\mathfrak{Q}/\mathfrak{p}} = 1.$$

If D is a normal subgroup of G, then $\mathfrak{p}$ is completely split in L^D.

Proof. We know that $[G : D] = g(\mathfrak{P}/\mathfrak{p})$ which is equal to $[L^D : K]$ by Galois theory. The previous proposition shows that $g(\mathfrak{P}/\mathfrak{Q}) = 1$ (recall that g counts how many primes are above). Now we compute that

$$\begin{aligned} e(\mathfrak{P}/\mathfrak{Q})f(\mathfrak{P}/\mathfrak{Q}) &= \frac{[L : L^D]}{g(\mathfrak{P}/\mathfrak{Q})} \\ &= [L : L^D] \\ &= \frac{[L : K]}{[L^D : K]}. \end{aligned}$$

Since we have that

$$[L : K] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})g(\mathfrak{P}/\mathfrak{p})$$

and $[L^D : K] = g(\mathfrak{P}/\mathfrak{p})$, we further get

$$\begin{aligned} e(\mathfrak{P}/\mathfrak{Q})f(\mathfrak{P}/\mathfrak{Q}) &= \frac{e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})g(\mathfrak{P}/\mathfrak{p})}{g(\mathfrak{P}/\mathfrak{p})} \\ &= e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) \\ &= e(\mathfrak{P}/\mathfrak{Q})f(\mathfrak{P}/\mathfrak{Q})e(\mathfrak{Q}/\mathfrak{p})f(\mathfrak{Q}/\mathfrak{p}) \end{aligned}$$

where the last equality comes from transitivity. Thus

$$e(\mathfrak{Q}/\mathfrak{p})f(\mathfrak{Q}/\mathfrak{p}) = 1$$

and $e(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{p}) = 1$ since they are positive integers.

If D is normal, we have that L^D/K is Galois. Thus

$$[L^D : K] = e(\mathfrak{Q}/\mathfrak{p})f(\mathfrak{Q}/\mathfrak{p})g(\mathfrak{Q}/\mathfrak{p}) = g(\mathfrak{Q}/\mathfrak{p})$$

and $\mathfrak{p}$ completely splits. □

Let σ be in D. Then σ induces an automorphism of $\mathcal{O}_L/\mathfrak{P}$ which fixes $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$. That is we get an element $\phi(\sigma) \in \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. We have thus constructed a map

$$\phi : D \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}).$$

This is a group homomorphism. We know that $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is cyclic, generated by the Frobenius automorphism defined by

$$\mathrm{Frob}_\mathfrak{P}(x) = x^q, \ q = |\mathbb{F}_\mathfrak{p}|.$$

Definition 3.7. The inertia group $I = I_{\mathfrak{P}/\mathfrak{p}}$ is defined as being the kernel of ϕ.

Example 3.6. Let $K = \mathbb{Q}(i)$ and $\mathcal{O}_K = \mathbb{Z}[i]$. We have that $K/\mathbb{Q}$ is a Galois extension, with Galois group $G = \{1, \sigma\}$ where $\sigma : a + ib \mapsto a - ib$.

- We have that
$$(2) = (1+i)^2\mathbb{Z}[i],$$
thus the ramification index is $e = 2$. Since $efg = n = 2$, we have that $f = g = 1$. The residue field is $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] = \mathbb{F}_2$. The decomposition group D is G since $\sigma((1+i)\mathbb{Z}[i]) = (1+i)\mathbb{Z}[i]$. Since $f = 1$, $\mathrm{Gal}(\mathbb{F}_2/\mathbb{F}_2) = \{1\}$ and $\phi(\sigma) = 1$. Thus the kernel of ϕ is $D = G$ and the inertia group is $I = G$.

- We have that
$$(13) = (2+3i)(2-3i),$$
thus the ramification index is $e = 1$. Here $D = 1$ for $(2 \pm 3i)$ since $\sigma((2+3i)\mathbb{Z}[i]) = (2-3i)\mathbb{Z}[i] \neq (2+3i)\mathbb{Z}[i]$. We further have that $g = 2$, thus $efg = 2$ implies that $f = 1$, which as for 2 implies that the inertia group is $I = G$. We have that the residue field for $(2 \pm 3i)$ is $\mathbb{Z}[i]/(2 \pm 3i)\mathbb{Z}[i] = \mathbb{F}_{13}$.

- We have that $(7)\mathbb{Z}[i]$ is inert. Thus $D = G$ (the ideal belongs to the base field, which is fixed by the whole Galois group). Since $e = g = 1$, the inertial degree is $f = 2$, and the residue field is $\mathbb{Z}[i]/(7)\mathbb{Z}[i] = \mathbb{F}_{49}$. The Galois group $\mathrm{Gal}(\mathbb{F}_{49}/\mathbb{F}_7) = \{1, \tau\}$ with $\tau : x \mapsto x^7$, $x \in \mathbb{F}_{49}$. Thus the inertia group is $I = \{1\}$.

We can prove that ϕ is surjective and thus get the following *exact sequence*:

$$1 \to I \to D \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) \to 1.$$

The decomposition group is so named because it can be used to decompose the field extension L/K into a series of intermediate extensions each of which has a simple factorization behavior at $\mathfrak{p}$. If we denote by L^I the fixed field of I, then the above exact sequence corresponds under Galois theory to the following

tower of fields:

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

Intuitively, this decomposition of the extension says that L^D/K contains all of the factorization of $\mathfrak{p}$ into distinct primes, while the extension L^I/L^D is the source of all the inertial degree in $\mathfrak{P}$ over $\mathfrak{p}$. Finally, the extension L/L^I is responsible for all of the ramification that occurs over $\mathfrak{p}$.

Note that the map ϕ plays a special role for further theories, including reciprocity laws and class field theory.

The main definitions and results of this chapter are

- Definition of discriminant, and that a prime ramifies if and only if it divides the discriminant.
- Definition of signature.
- The terminology relative to ramification: prime above/below, inertial degree, ramification index, residue field, ramified, inert, totally ramified, split.
- The method to compute the factorization if $\mathcal{O}_K = \mathbb{Z}[\theta]$.
- The formula $[L : K] = \sum_{i=1}^{g} e_i f_i$.
- The notion of absolute and relative extensions.
- If L/K is Galois, that the Galois group acts transitively on the primes above a given $\mathfrak{p}$, that $[L : K] = efg$, and the concepts of decomposition group and inertia group.

Chapter 4

Ideal Class Group and Units

We are now interested in understanding two aspects of ring of integers of number fields: "how principal they are" (that is, what is the proportion of principal ideals among all the ideals), and what is the structure of their group of units. For the former task, we will introduce the notion of class number (as the measure of how principal a ring of integers is), and prove that the class number is finite. We will then prove Dirichlet's Theorem for the structure of groups of units. Both results will be derived in the spirit of "geometry of numbers", that is as a consequence of Minkowski's theorem, where algebraic results are proved thanks to a suitable geometrical interpretation (mainly the fact that a ring of integers can be seen as a lattice in $\mathbb{R}^n$ via the n embeddings of its number field).

4.1 Ideal class group

Let K be a number field, and $\mathcal{O}_K$ be its ring of integers. We have seen in Chapter 2 that we can extend the notion of ideal to fractional ideal, and that with this new notion, we have a group structure (Theorem 2.5). Let I_K denote the group of fractional ideals of K. Let P_K denote the subgroup of I_K formed by the principal ideals, that is ideals of the form $\alpha\mathcal{O}_K$, $\alpha \in K^\times$.

Definition 4.1. The ideal class group, denoted by $\mathrm{Cl}(K)$, is

$$\mathrm{Cl}(K) = I_K/P_K.$$

Definition 4.2. We denote by h_K the cardinality $|\mathrm{Cl}_K|$, called the class number.

In particular, if $\mathcal{O}_K$ is a principal ideal domain, then $\mathrm{Cl}(K) = 0$, and $h_K = 1$.

Our goal is now to prove that the class number is finite for ring of integers of number fields. The lemma below is a version of Minkowski's theorem.

Lemma 4.1. *Let Λ be a lattice of $\mathbb{R}^n$. Let $X \subset \mathbb{R}^n$ be a convex, compact set (that is a closed and bounded set since we are in $\mathbb{R}^n$), which is symmetric with respect to 0 (that is, $x \in X \iff -x \in X$). If*

$$\mathrm{Vol}(X) \geq 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda),$$

then there exists $0 \neq \lambda \in \Lambda$ such that $\lambda \in X$.

Proof. Let us first assume that the inequality is strict: $\mathrm{Vol}(X) > 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. Let us consider the map

$$\psi : \frac{1}{2}X = \{\frac{x}{2} \in \mathbb{R}^n \mid x \in X\} \to \mathbb{R}^n/\Lambda.$$

If ψ were injective, then

$$\mathrm{Vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{Vol}(X) \leq \mathrm{Vol}(\mathbb{R}^n/\Lambda)$$

that is $\mathrm{Vol}(X) \leq 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$, which contradicts our assumption. Thus ψ cannot be injective, which means that there exist $x_1 \neq x_2 \in \frac{1}{2}X$ such that $\psi(x_1) = \psi(x_2)$. By symmetry, we have that $-x_2 \in \frac{1}{2}X$, and by convexity of X (that is $(1-t)x + ty \in X$ for $t \in [0,1]$), we have that

$$\left(1 - \frac{1}{2}\right) x_1 + \frac{1}{2}(-x_2) = \frac{x_1 - x_2}{2} \in \frac{1}{2}X.$$

Thus $0 \neq \lambda = x_1 - x_2 \in X$, and $\lambda \in \Lambda$ (since $\psi(x_1 - x_2) = 0$).

Let us now assume that $\mathrm{Vol}(X) = 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. By what we have just proved, there exists $0 \neq \lambda_\epsilon \in \Lambda$ such that $\lambda_\epsilon \in (1+\epsilon)X$ for all $\epsilon > 0$, since

$$\begin{aligned} \mathrm{Vol}((1+\epsilon)X) &= (1+\epsilon)^n \mathrm{Vol}(X) \\ &= (1+\epsilon)^n 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda) \\ &> 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda), \text{ for all } \epsilon > 0. \end{aligned}$$

In particular, if $\epsilon < 1$, then $\lambda_\epsilon \in 2X \cap \Lambda$. The set $2X \cap \Lambda$ is compact and discrete (since Λ is discrete), it is thus finite. Let us now understand what is happening here. On the one hand, we have a sequence λ_ϵ with infinitely many terms since there is one for every $0 < \epsilon < 1$, while on the other hand, those infinitely many terms are all lattice points in $2X$, which only contains finitely many of them. This means that this sequence must converge to a point $0 \neq \lambda \in \Lambda$ which belongs to $(1+\epsilon)X$ for infinitely many $\epsilon > 0$. Thus $\lambda \in \Lambda \cap (\cap_{\epsilon \to 0}(1+\epsilon)X - 0)$. Since X is closed, we have that $\lambda \in X$. □

Let $n = [K : \mathbb{Q}]$ be the degree of K and let (r_1, r_2) be the signature of K. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the r_1 real embeddings of K into $\mathbb{R}$. We choose one of the two embeddings in each pair of complex embeddings, which we denote by

$\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$. We consider the following map, called canonical embedding of K:

$$\begin{aligned} \sigma : \quad K &\to \quad \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \simeq \mathbb{R}^n \\ \alpha &\mapsto \quad (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)). \end{aligned} \tag{4.1}$$

We have that the image of $\mathcal{O}_K$ by σ is a lattice $\sigma(\mathcal{O}_K)$ in $\mathbb{R}^n$ (we have that $\sigma(\mathcal{O}_K)$ is a free abelian group, which contains a basis of $\mathbb{R}^n$). Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Let M be the generator matrix of the lattice $\sigma(\mathcal{O}_K)$, given by

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_{r_1}(\alpha_1) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \dots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_1)) & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \vdots & & & & & & \vdots & \\ \sigma_1(\alpha_n) & \dots & \sigma_{r_1}(\alpha_n) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \dots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_n)) & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{pmatrix}$$

whose determinant is given by

$$\mathrm{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K)) = |\det(M)| = \frac{\sqrt{|\Delta_K|}}{2^{r_2}}.$$

Indeed, we have that $\mathrm{Re}(x) = (x + \bar{x})/2$ and $\mathrm{Im}(x) = (x - \bar{x})/2i$, $x \in \mathbb{C}$, and

$$|\det(M)| = |\det(M')|$$

where M' is given by

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \frac{\sigma_{r_1+1}(\alpha_1) - \overline{\sigma_{r_1+1}(\alpha_1)}}{2i} & \dots & \sigma_{r_1+r_2}(\alpha_1) & \frac{\sigma_{r_1+r_2}(\alpha_1) - \overline{\sigma_{r_1+r_2}(\alpha_1)}}{2i} \\ \vdots & & & & & & \vdots & \\ \sigma_1(\alpha_n) & \dots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \frac{\sigma_{r_1+1}(\alpha_n) - \overline{\sigma_{r_1+1}(\alpha_n)}}{2i} & \dots & \sigma_{r_1+r_2}(\alpha_n) & \frac{\sigma_{r_1+r_2}(\alpha_n) - \overline{\sigma_{r_1+r_2}(\alpha_n)}}{2i} \end{pmatrix}.$$

Again, we have that $|\det(M')| = 2^{-r_2}|\det(M'')|$, with M'' given by this time

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_1) & \overline{\sigma_{r_1+r_2}(\alpha_1)} \\ \vdots & & & & & & \vdots & \\ \sigma_1(\alpha_n) & \dots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \overline{\sigma_{r_1+1}(\alpha_n)} & \dots & \sigma_{r_1+r_2}(\alpha_n) & \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{pmatrix},$$

which concludes the proof, since (recall that complex embeddings come by pairs of conjugates)

$$|\det(M)| = 2^{-r_2}|\det(M'')| = 2^{-r_2}\sqrt{\Delta_K}.$$

We are now ready to prove that $\mathrm{Cl}(K) = I_K/P_K$ is finite.

Theorem 4.2. *Let K be a number field with discriminant Δ_K.*

1. *There exists a constant $C = C_{r_1,r_2} > 0$ (which only depends on r_1 and r_2) such that every ideal class (that is every coset of $\mathrm{Cl}(K)$) contains an integral ideal whose norm is at most*

$$C\sqrt{|\Delta_K|}.$$

2. The group $\mathrm{Cl}(K)$ *is finite.*

Proof. Recall first that by definition, a non-zero fractional ideal J is a finitely generated $\mathcal{O}_K$-submodule of K, and there exists $\beta \in K^\times$ such that $\beta J \subset \mathcal{O}_K$ (if β_i span J as $\mathcal{O}_K$-module, write $\beta_i = \delta_i/\gamma_i$ and set $\beta = \prod \gamma_i$). The fact that $\beta J \subset \mathcal{O}_K$ exactly means that $\beta \in J^{-1}$ by definition of the inverse of a fractional ideal (see Chapter 2). The idea of the proof consists of, given a fractional ideal J, looking at the norm of a corresponding integral ideal βJ, which we will prove is bounded as claimed.

Let us pick a non-zero fractional ideal I. Since I is a finitely generated $\mathcal{O}_K$-module, we have that $\sigma(I)$ is a lattice in $\mathbb{R}^n$, and so is $\sigma(I^{-1})$, with the property that

$$\mathrm{Vol}(\mathbb{R}^n/\sigma(I^{-1})) = \mathrm{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K))\mathrm{N}(I^{-1}) = \frac{\sqrt{|\Delta_K|}}{2^{r_2}\mathrm{N}(I)},$$

where the first equality comes from the fact that the volume is given by the determinant of the generator matrix of the lattice. Now since we have two lattices, we can write the generator matrix of $\sigma(I^{-1})$ as being the generator matrix of $\sigma(\mathcal{O}_K)$ multiplied by a matrix whose determinant in absolute value is the index of the two lattices. Let X be a compact convex set, symmetrical with respect to 0. In order to get a set of volume big enough to use Minkowski theorem, we set a scaling factor

$$\lambda^n = 2^n \frac{\mathrm{Vol}(\mathbb{R}^n/\sigma(I^{-1}))}{\mathrm{Vol}(X)},$$

so that the volume of λX is

$$\mathrm{Vol}(\lambda X) = \lambda^n \mathrm{Vol}(X) = 2^n \mathrm{Vol}(\mathbb{R}^n/\sigma(I^{-1})).$$

By Lemma 4.1, there exists $0 \neq \sigma(\alpha) \in \sigma(I^{-1})$ and $\sigma(\alpha) \in \lambda X$. Since $\alpha \in I^{-1}$, we have that αI is an integral ideal in the same ideal class as I, and

$$\mathrm{N}(\alpha I) = |N_{K/\mathbb{Q}}(\alpha)|\mathrm{N}(I) = |\prod_{i=1}^{n} \sigma_i(\alpha)|\mathrm{N}(I) \leq M\lambda^n \mathrm{N}(I),$$

where $M = \max_{x \in X} \prod |x_i|$, $x = (x_1, \ldots, x_n)$, so that the maximum over λX gives $\lambda^n M$. Thus, by definition of λ^n, we have that

$$\begin{aligned} \mathrm{N}(\alpha I) &\leq \frac{2^n \mathrm{Vol}(\mathbb{R}^n/\sigma(I^{-1}))}{\mathrm{Vol}(X)} M\mathrm{N}(I) \\ &= \frac{2^n M}{2^{r_2}\mathrm{Vol}(X)} \sqrt{\Delta_K} \\ &= \underbrace{\frac{2^{r_1+r_2} M}{\mathrm{Vol}(X)}}_{C} \sqrt{\Delta_K}. \end{aligned}$$

This completes the first part of the proof.

Figure 4.1: Johann Peter Gustav Lejeune Dirichlet (1805-1859)

We are now left to prove that $\mathrm{Cl}(K)$ is a finite group. By what we have just proved, we can find a system of representatives J_i of I_K/P_K consisting of integral ideals J_i, of norm smaller than $C\sqrt{|\Delta_K|}$. In particular, the prime factors of J_i have a norm smaller than $C\sqrt{|\Delta_K|}$. Above the prime numbers $p < C\sqrt{|\Delta_K|}$, there are only finitely many prime ideals (or in other words, there are only finitely many integrals with a given norm). □

4.2 Dirichlet Units Theorem

By abuse of language, we call units of K the units of $\mathcal{O}_K$, that is the invertible elements of $\mathcal{O}_K$. We have seen early on (Corollary 1.11) that units are characterized by their norm, namely units are exactly the elements of $\mathcal{O}_K$ with norm ± 1.

Theorem 4.3. (Dirichlet Units Theorem.) *Let K be a number field of degree n, with signature (r_1, r_2). The group $\mathcal{O}_K^*$ of units of K is the product of the group $\mu(\mathcal{O}_K)$ of roots of unity in $\mathcal{O}_K$, which is cyclic and finite, and a free group on $r_1 + r_2 - 1$ generators. In formula, we have that*

$$\mathcal{O}_K^* \simeq \mathbb{Z}^{r_1+r_2-1} \times \mu(\mathcal{O}_K).$$

The most difficult part of this theorem is actually to prove that the free group has exactly $r_1 + r_2 - 1$ generators. This is nowadays usually proven using Minkowski's theorem. Dirichlet though did not have Minkowski's theorem available: he proved the unit theorem in 1846 while Minkowski developed the geometry of numbers only around the end of the 19th century. He used instead the pigeonhole principle. It is said that Dirichlet got the main idea for his proof while attending a concert in the Sistine Chapel.

Proof. Let $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ be the canonical embedding of K (see (4.1)). The logarithmic embedding of K is the mapping

$$\begin{aligned} \lambda : \quad K^* &\to \quad \mathbb{R}^{r_1+r_2} \\ \alpha &\mapsto \quad (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_{r_1+r_2}(\alpha))|. \end{aligned}$$

Since $\lambda(\alpha\beta) = \lambda(\alpha)+\lambda(\beta)$, λ is a homomorphism from the multiplicative group K^* to the additive group of $\mathbb{R}^{r_1+r_2}$.

Step 1. We first prove that the kernel of λ restricted to $\mathcal{O}_K^*$ is a finite group. In order to do so, we prove that if C is a bounded subset of $\mathbb{R}^{r_1+r_2}$, then $C' = \{x \in \mathcal{O}_K^*,\ \lambda(x) \in C\}$ is a finite set. In words, we look at the preimage of a bounded set by the logarithmic embedding (more precisely, at the restriction of the preimage to the units of $\mathcal{O}_K$).

Proof. Since C is bounded, all $|\sigma_i(x)|$, $x \in \mathcal{O}_K^*$, $i = 1, \ldots, n$ belong to some interval say $[a^{-1}, a]$, $a > 1$. Thus the elementary polynomials in the $\sigma_i(x)$ will also belong to some interval of the same form. Now they are the coefficients of the characteristic polynomial of x, which has integer coefficients since $x \in \mathcal{O}_K^*$. Thus there are only finitely many possible characteristic polynomials of elements $x \in C'$, hence only finitely many possible roots of minimal polynomials of elements $x \in C'$, which shows that x can belong to C' for only finitely many x. Now if we set $C = \{0\}$, C' is the kernel $\ker(\lambda)|_{\mathcal{O}_K^*}$ of λ restricted to $\mathcal{O}_K^*$ and is thus finite.

Step 2. We now show that $\ker(\lambda)|_{\mathcal{O}_K^*}$ consists of exactly all the roots of unity $\mu(\mathcal{O}_K)$.

Proof. That it does consist of roots of unity (and is cyclic) is a known property of any subgroup of the multiplicative group of any field. Thus if $x \in \ker(\lambda)|_{\mathcal{O}_K^*}$ then x is a root of unity. Now conversely, suppose that $x^m = 1$. Then x is an algebraic integer, and

$$|\sigma_i(x)|^m = |\sigma_i(x^m)| = |1| = 1$$

so that $|\sigma_i(x)| = 1$, and thus $\log|\sigma_i(x)| = 0$ for all i, showing that $x \in \ker(\lambda)|_{\mathcal{O}_K^*}$.

Step 3. We are now ready to prove that $\mathcal{O}_K^*$ is a finite generated abelian group, isomorphic to $\mu(\mathcal{O}_K) \times \mathbb{Z}^s$, $s \leq r_1 + r_2$.

Proof. By Step 1, we know that $\lambda(\mathcal{O}_K^*)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$, that is, any bounded subset of $\mathbb{R}^{r_1+r_2}$ contains only finitely many points of $\lambda(\mathcal{O}_K^*)$. Thus $\lambda(\mathcal{O}_K^*)$ is a lattice in $\mathbb{R}^s$, hence a free $\mathbb{Z}$-module of rank s, for some $s \leq r_1 + r_2$. Now by the first isomorphism theorem, we have that

$$\lambda(\mathcal{O}_K^*) \simeq \mathcal{O}_K^*/\mu(\mathcal{O}_K)$$

with $\lambda(x)$ corresponding to the coset $x\mu(\mathcal{O}_K)$. If $x_1\mu(\mathcal{O}_K), \ldots, x_s\mu(\mathcal{O}_K)$ form a basis for $\mathcal{O}_K^*/\mu(\mathcal{O}_K)$ and $x \in \mathcal{O}_K^*$, then $x\mu(\mathcal{O}_K)$ is a finite produce of powers of the x_iG, so x is an element of $\mu(\mathcal{O}_K)$ times a finite product of powers of the x_i. Since the $\lambda(x_i)$ are linearly independent, so are the x_i (provided that the notion of linear independence is translated to a multiplicative setting: $x_1, \ldots, x_s$ are multiplicatively independent if $x_1^{m_1} \cdots x_s^{m_s} = 1$ implies that $m_i = 0$ for all i,

from which it follows that $x_1^{m_1}\cdots x_s^{m_s} = x_1^{n_1}\cdots x_s^{n_s}$ implies $m_i = n_i$ for all i). The result follows.

Step 4. We now improve the estimate of s and show that $s \leq r_1 + r_2 - 1$.
Proof. If x is a unit, then we know that its norm must be ± 1. Then

$$\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)}.$$

By taking the absolute values and applying the logarithmic embedding, we get

$$0 = \sum_{i=1}^{r_1} \log|\sigma_i(x)| + \sum_{j=r_1+1}^{r_1+r_2} \log(|\sigma_j(x)||\overline{\sigma_j(x)}|)$$

and $\lambda(x) = (y_1, \ldots, y_{r_1+r_2})$ lies in the hyperplane W whose equation is

$$\sum_{i=1}^{r_1} y_i + 2\sum_{j=r_1+1}^{r_1+r_2} y_j = 0.$$

The hyperplane has dimension r_1+r_2-1, so as above, $\lambda(\mathcal{O}_K^*)$ is a free $\mathbb{Z}$-module of rank $s \leq r_1 + r_2 - 1$.

Step 5. We are left with showing that $s = r_1 + r_2 - 1$, which is actually the hardest part of the proof. This uses Minkowski theorem. The proof may come later... one proof can be found in the online lecture of Robert Ash. □

Example 4.1. Consider K an imaginary quadratic field, that is of the form $K = \mathbb{Q}(\sqrt{-d})$, with d a positive square free integer. Its signature is $(r_1, r_2) = (0, 1)$. We thus have that its group of units is given by

$$\mathbb{Z}^{r_1+r_2-1} \times G = G,$$

that is only roots of unity. Actually, we have that the units are the 4rth roots of unity if $K = \mathbb{Q}(\sqrt{-1})$ (that is $\pm 1, \pm i$), the 6th roots of unity if $K = \mathbb{Q}(\sqrt{-3})$ (that is $\pm 1, \pm\zeta_3, \pm\zeta_3^2$), and only ± 1 otherwise.

Example 4.2. For $K = \mathbb{Q}(\sqrt{3})$, we have $(r_1, r_2) = (2, 0)$, thus $r_1 + r_2 - 1 = 1$, and $\mu(\mathcal{O}_K) = \pm 1$. The unit group is given by

$$\mathcal{O}_K^* \simeq \pm(2 + \sqrt{3})^{\mathbb{Z}}.$$

The main definitions and results of this chapter are

- Definition of ideal class group and class number.
- The fact that the class number of a number field is finite.
- The structure of units in a number field (the statement of Dirichlet's theorem)

Chapter 5

p-adic numbers

The p-adic numbers were first introduced by the German mathematician K. Hensel (though they are foreshadowed in the work of his predecessor E. Kummer). It seems that Hensel's main motivation was the analogy between the ring of integers $\mathbb{Z}$, together with its field of fractions $\mathbb{Q}$, and the ring $\mathbb{C}[X]$ of polynomials with complex coefficients, together with its field of fractions $\mathbb{C}(X)$. Both $\mathbb{Z}$ and $\mathbb{C}[X]$ are rings where there is unique factorization: any integer can be expressed as a product of primes, and any polynomial can be expressed uniquely as

$$P(X) = a(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n),$$

where a and $\alpha_1, \dots, \alpha_n$ are complex numbers. This is the main analogy Hensel explored: the primes $p \in \mathbb{Z}$ are analogous to the linear polynomials $X - \alpha \in \mathbb{C}[X]$. Suppose we are given a polynomial $P(X)$ and $\alpha \in \mathbb{C}$, then it is possible (for example using a Taylor expansion) to write the polynomial in the form

$$P(X) = \sum_{i=0}^{n} a_i (X - \alpha)^i, \ a_i \in \mathbb{C}.$$

This also works naturally for the integers: given a positive integer m and a prime p, we can write it "in base p", that is

$$m = \sum_{i=0}^{n} a_i p^i, \ a_i \in \mathbb{Z}$$

and $0 \leq a_i \leq p - 1$.

The reason such expansions are interesting is that they give "local" information: the expansion in powers of $(X - \alpha)$ shows if $P(X)$ vanishes at α, and to what order. Similarly, the expansion in base p will show if m is divisible by p, and to what order.

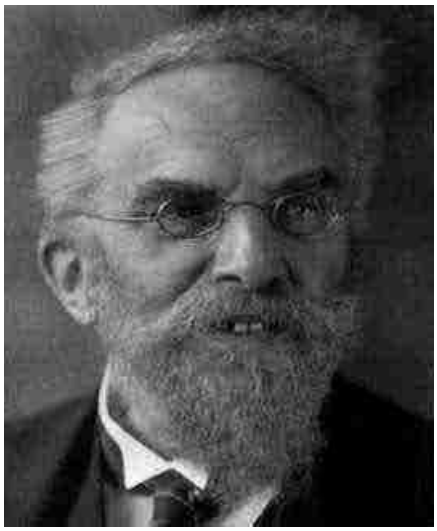


Figure 5.1: Kurt Hensel (1861-1941)

Now for polynomials, one can go a little further, and consider their Laurent expansion

$$f(X) = \sum_{i \geq n_0} a_i (X - \alpha)^i,$$

that is any rational function can be expanded into a series of this kind in terms of each of the "primes" $(X - \alpha)$. From an algebraic point of view, we have two fields: $\mathbb{C}(X)$ of all rational functions, and another field $\mathbb{C}((X - \alpha))$ which consists of all Laurent series in $(X - \alpha)$. Then the function

$$f(X) \mapsto \text{ expansion around } (X - \alpha)$$

defines an inclusion of fields

$$\mathbb{C}(X) \to \mathbb{C}((X - \alpha)).$$

Hensel's idea was to extend the analogy between $\mathbb{Z}$ and $\mathbb{C}[X]$ to include the construction of such expansions. Recall that the analogous of choosing α is choosing a prime number p. We already know the expansion for a positive integer m, it is just the base p representation. This can be extended for rational numbers

$$x = \frac{a}{b} = \sum_{n \geq n_0} a_n p^n$$

yielding for every rational number x a finite-tailed Laurent series in powers of p, which is called a *p-adic expansion* of x.

We will come back to this construction in this chapter, and also see that it achieves Hensel's goal, since the set of all finite-tailed Laurent series in powers of p is a field, denoted by $\mathbb{Q}_p$, and that we similarly get a function

$$f(X) \mapsto \text{ expansion around } (X - \alpha)$$

which defines an inclusion of fields

$$\mathbb{Q} \to \mathbb{Q}_p.$$

Of course, more formalism has been further introduced since Hensel's idea, which will be presented in this chapter.

5.1 p-adic integers and p-adic numbers

We start this chapter by introducing p-adic integers, both intuitively by referring to writing an integer in a given base p, and formally by defining the concept of inverse limit. This latter approach will allow to show that p-adic integers form a ring, denoted by $\mathbb{Z}_p$. We will then consider "fractions" of p-adic integers, that is p-adic numbers, which we will show form the field $\mathbb{Q}_p$.

Let p be a prime number. Given an integer $n > 0$, we can write n in base p:

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$$

with $0 \leq a_i < p$.

Definition 5.1. A p-adic integer is a (formal) serie

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$$

with $0 \leq a_i < p$.

The set of p-adic integers is denoted by $\mathbb{Z}_p$. If we cut an element $\alpha \in \mathbb{Z}_p$ at its kth term

$$\alpha_k = a_0 + a_1 p + \cdots + a_{k-1} p^{k-1}$$

we get a well defined element of $\mathbb{Z}/p^k\mathbb{Z}$. This yields mappings

$$\mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}.$$

A sequence of α_k, $k > 0$, such that $\alpha_k \mod p^{k'} \equiv \alpha_{k'}$ for all $k' < k$ defines a unique p-adic integer $\alpha \in \mathbb{Z}_p$ (start with $k = 1$, $\alpha_1 = a_0$, then for $k = 2$, we need to have $\alpha_2 = a_0 + a_1 p$ for it to be a partial sum coherent with α_1). We thus have the following bijection:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}.$$

The notation on the right hand side is called inverse limit. Here we have an inverse limit of rings (since $\mathbb{Z}/p^k\mathbb{Z}$ is a ring). The formal definition of an inverse

limit involves more formalism than we need for our purpose. To define an inverse limit of rings, we need a sequence of rings, which is suitably indexed (here the sequence $\mathbb{Z}/p^k\mathbb{Z}$ is indexed by the integer k). We further need a sequence of ring homomorphisms π_{ij} with the same index (here π_{ij} with i and j integers, $i \leq j$) satisfying that

1. π_{ii} is the identity on the ring indexed by i for all i,
2. for all i, j, k, $i \leq j \leq k$, we have $\pi_{ij} \circ \pi_{jk} = \pi_{ik}$.

In our case, $\pi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ is the natural projection for $i \leq j$, and the inverse limit of rings we consider is defined by

$$\lim_{\leftarrow} \mathbb{Z}/p^i\mathbb{Z} = \{(x_i)_i \in \prod_i \mathbb{Z}/p^i\mathbb{Z} \mid \pi_{ij}(x_j) = x_i,\ i \leq j\}.$$

Example 5.1. We can write -1 as a p-adic integer:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots$$

The description of $\mathbb{Z}_p$ as limit of $\mathbb{Z}/p^k\mathbb{Z}$ allows to endow $\mathbb{Z}_p$ with a commutative ring structure: given $\alpha, \beta \in \mathbb{Z}_p$, we consider their sequences $\alpha_k, \beta_k \in \mathbb{Z}/p^k\mathbb{Z}$. We then form the sequence $\alpha_k + \beta_k \in \mathbb{Z}/p^k\mathbb{Z}$ which yields a well defined element $\alpha + \beta \in \mathbb{Z}_p$. We do the same for multiplication.

Example 5.2. Let us compute the sum of $\alpha = 2+1\cdot 3+\dots$ and $\beta = 1+2\cdot 3+\dots$ in $\mathbb{Z}_3$. We have $\alpha_1 \equiv 2 \mod 3$ and $\beta_1 \equiv 1 \mod 3$, thus

$$(\alpha + \beta)_1 = \alpha_1 + \beta_1 \equiv 0 \mod 3.$$

Then $\alpha_2 \equiv 5 \mod 3^2$ and $\beta_2 \equiv 7 \mod 3^2$, so that

$$(\alpha + \beta)_2 = \alpha_2 + \beta_2 = 12 \equiv 3 \mod 3^2.$$

This yields

$$\alpha + \beta = 0 + 1 \cdot 3 + \dots \in \mathbb{Z}_3.$$

We are just computing the addition in base 3!

Note that $\mathbb{Z}$ is included in $\mathbb{Z}_p$.

Let us now look at fractions instead of integers. The fraction $-3/2$ is the solution of the equation $2x + 3 = 0$. Does this equation have a solution in $\mathbb{Z}_3$? We have that

$$\frac{3}{-2} = \frac{3}{1-3} = 3(1 + 3 + 3^2 + \dots)$$

since

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots .$$

Thus

$$\frac{3}{-2} = 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \dots$$

Actually, if $x = a/b$ and p does not divide b, then $x = a/b \in \mathbb{Z}_p$. Indeed, there is an inverse $b^{-1} \in \mathbb{Z}/p^k\mathbb{Z}$ and the sequence ab^{-1} converges towards an $x \in \mathbb{Z}_p$ such that $bx = a$. On the contrary, $1/p \notin \mathbb{Z}_p$, since for all $x \in \mathbb{Z}_p$, we have that $(px)_1 = 0 \neq 1$.

Definition 5.2. The *p*-adic numbers are series of the form

$$a_{-n}\frac{1}{p^n} + a_{-n+1}\frac{1}{p^{n-1}} + \cdots + a_{-1}\frac{1}{p} + a_0 + a_1 p + \dots$$

The set of p-adic numbers is denoted by $\mathbb{Q}_p$. It is a field. We have an inclusion of $\mathbb{Q}$ into $\mathbb{Q}_p$. Indeed, if $x \in \mathbb{Q}$, then there exists $N \geq 0$ such that $p^N x \in \mathbb{Z}_p$. In other words, $\mathbb{Q}$ can be seen as a subfield of $\mathbb{Q}_p$.

Example 5.3. Let $p = 7$. Consider the equation

$$X^2 - 2 = 0$$

in $\mathbb{Z}_7$. Let $\alpha = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \dots$ be the solution of the equation. Then we have that $a_0^2 - 2 \equiv 0 \mod 7$. We thus two possible values for a_0:

$$\alpha_1 = a_0 = 3,\ \alpha_1 = a_0 = 4.$$

We will see that those two values will give two solutions to the equation. Let us choose $a_0 = 3$, and set

$$\alpha_2 = a_0 + a_1 \cdot 7 \in \mathbb{Z}/49\mathbb{Z}.$$

We have that

$$\begin{aligned}
\alpha_2^2 - 2 \equiv 0 \mod 7^2 &\iff a_0^2 + a_1^2 \cdot 7^2 + 2 \cdot 7 a_0 a_1 - 2 \equiv 0 \mod 7^2 \\
&\iff 3^2 + 2 \cdot 3 \cdot 7 \cdot a_1 - 2 \equiv 0 \mod 7^2 \\
&\iff 7 + 6 \cdot 7 \cdot a_1 \equiv 0 \mod 7^2 \\
&\iff 1 + 6 \cdot a_1 \equiv 0 \mod 7 \\
&\iff a_1 \equiv 1 \mod 7.
\end{aligned}$$

By iterating the above computations, we get that

$$\alpha = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 + \dots$$

The other solution is given by

$$\alpha = 4 + 5 \cdot 7 + 4 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + \dots$$

Note that $X^2 - 2$ does not have solutions in $\mathbb{Q}_2$ or in $\mathbb{Q}_3$.

In the above example, we solve an equation in the p-adic integers by solving each coefficient one at a time modulo p, p^2, ... If there is no solution for one coefficient with a given modulo, then there is no solution for the equation, as this is the case for $\mathbb{Q}_2$ or $\mathbb{Q}_3$.

In the similar spirit, we can consider looking for roots of a given equation in $\mathbb{Q}$. If there are roots in $\mathbb{Q}$, then there are also roots in $\mathbb{Q}_p$ for every $p \leq \infty$ (that is, in all the $\mathbb{Q}_p$ and in $\mathbb{R}$). Hence we can conclude that there are no rational roots if there is some $p \leq \infty$ for which there are no p-adic roots. The fact that roots in $\mathbb{Q}$ automatically are roots in $\mathbb{Q}_p$ for every p means that a "global" root is also a "local" root "everywhere" (that is at each p).

Much more interesting would be a converse: that "local" roots could be "patched together" to give a "global root". That putting together local information at all $p \leq \infty$ should give global information is the idea behind the so-called local-global principle, first clearly stated by Hasse. A good example where this principle is successful is the Hasse-Minkowski theorem:

Theorem 5.1. *(***Hasse-Minkowski***)* *Let $F(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ be a quadratic form (that is a homogeneous polynomial of degree 2 in n variables). The equation*

$$F(X_1, \ldots, X_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$.

5.2 The p-adic valuation

We now introduce the notion of p-adic valuation and p-adic absolute value. We first define them for elements in $\mathbb{Q}$, and extend them to elements in $\mathbb{Q}_p$ after proving the so-called product formula. The notion of absolute value on $\mathbb{Q}_p$ enables to define Cauchy sequences, and we will see that $\mathbb{Q}_p$ is actually the completion of $\mathbb{Q}$ with respect to the metric induced by this absolute value.

Let α be a non-zero element of $\mathbb{Q}$. We can write it as

$$\alpha = p^k \frac{g}{h},\ k \in \mathbb{Z},$$

and g, h, p coprime to each other, with p prime. We set

$$\begin{aligned} \mathrm{ord}_p(\alpha) &= k \\ |\alpha|_p &= p^{-k} \\ \mathrm{ord}_p(0) &= \infty \\ |0|_p &= 0. \end{aligned}$$

We call $\mathrm{ord}_p(\alpha)$ the p-adic valuation of α and $|\alpha|_p$ the p-adic absolute value of α. We have the following properties for the p-adic valuation:

$$\begin{aligned} \mathrm{ord}_p : \mathbb{Q} &\to \mathbb{Z} \cup \{\infty\} \\ \mathrm{ord}_p(ab) &= \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \\ \mathrm{ord}_p(a+b) &\geq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b)) \\ \mathrm{ord}_p(a) = \infty &\iff a = 0. \end{aligned}$$

Let us now look at some properties of the p-adic absolute value:

$$\begin{array}{rcl} |\cdot|_p : \mathbb{Q} & \to & \mathbb{R}_{\geq 0} \\ |ab|_p & = & |a|_p |b|_p \\ |a+b|_p & \leq & \max(|a|_p, |b|_p) \leq |a|_p + |b|_p \\ |a|_p = 0 & \iff & a = 0. \end{array}$$

Note that in a sense, we are just trying to capture for this new absolute value the important properties of the usual absolute value. Now the p-adic absolute value induces a metric on $\mathbb{Q}$, by setting

$$d_p(a,b) = |a-b|_p,$$

which is indeed a distance (it is positive: $d_p(a,b) \geq 0$ and is 0 if and only if $a = b$, it is symmetric: $d_p(a,b) = d_p(b,a)$, and it satisfies the triangle inequality: $d_p(a,c) \leq d_p(a,b) + d_p(b,c)$). With that metric, two elements a and b are close if $|a-b|_p$ is small, which means that $\mathrm{ord}_p(a-b)$ is big, or in other words, a big power of p divides $a-b$.

The following result connects the usual absolute value of $\mathbb{Q}$ with the p-adic absolute values.

Lemma 5.2. (Product Formula) *Let $0 \neq \alpha \in \mathbb{Q}$. Then*

$$\prod_{\nu} |\alpha|_\nu = 1$$

where $\nu \in \{\infty, 2, 3, 5, 7, \ldots\}$ and $|\alpha|_\infty$ is the real absolute value of α.

Proof. We prove it for α a positive integer, the general case will follow. Let α be a positive integer, which we can factor as

$$\alpha = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Then we have

$$\begin{cases} |\alpha|_q = 1 & \text{if } q \neq p_i \\ |\alpha|_{p_i} = p_i^{-a_i} & \text{for } i = 1, \ldots, k \\ |\alpha|_\infty = p_1^{a_1} \cdots p_k^{a_k} \end{cases}$$

The result follows. □

In particular, if we know all but one absolute value, the product formula allows us to determine the missing one. This turns out to be surprisingly important in many applications. Note that a similar result is true for finite extensions of $\mathbb{Q}$, except that in that case, we must use several "infinite primes" (actually one for each different inclusion into $\mathbb{R}$ and $\mathbb{C}$). We will come back to this result in the next chapter.

The set of primes together with the "infinite prime", over which the product is taken in the product formula, is usually called the set of places of $\mathbb{Q}$.

Definition 5.3. The set

$$\mathcal{M}_{\mathbb{Q}} = \{\infty, 2, 3, \ldots\}$$

is the set of places of $\mathbb{Q}$.

Let us now get back to the p-adic numbers. Let $\alpha = a_k p^k + a_{k+1}p^{k+1} + a_{k+2}p^{k+2} + \ldots \in \mathbb{Q}_p$, with $a_k \neq 0$, and k possibly negative. We then set

$$\begin{aligned} \mathrm{ord}_p(\alpha) &= k \\ |\alpha|_p &= p^{-k}. \end{aligned}$$

This is an extension of the definition of absolute value defined for elements of $\mathbb{Q}$.

Before going on further, let us recall two definitions:

- Recall that a sequence of elements x_n in a given field is called a Cauchy sequence if for every $\epsilon > 0$ one can find a bound M such that we have $|x_n - x_m| < \epsilon$ whenever $m, n \geq M$.
- A field K is called complete with respect to an absolute value $|\cdot|$ if every Cauchy sequence of elements of K has a limit in K.

Let $\alpha \in \mathbb{Q}_p$. Recall that α_l is the integer $0 \leq \alpha_l < p^l$ obtained by cutting α after $a_{l-1}p^{l-1}$. If $n > m$, we have

$$\begin{aligned} |\alpha_n - \alpha_m|_p &= |a_k p^k + \ldots + a_m p^m + \ldots + a_{n-1}p^{n-1} - a_k p^k - \ldots - a_{m-1}p^{m-1}| \\ &= |a_m p^m + a_{m+1}p^{m+1} + \ldots + a_{n-1}p^{n-1}|_p \leq p^{-m}. \end{aligned}$$

This expression tends to 0 when m tends to infinity. In other words, the sequence $(\alpha_n)_{n\geq 0}$ is a Cauchy sequence with respect to the metric induced by $|\cdot|_p$.

Now let $(\alpha_n)_{n\geq 1}$ be a Cauchy sequence, that is $|\alpha_n - \alpha_m|_p \to 0$ when $m \to \infty$ with $n > m$, that is, $\alpha_n - \alpha_m$ is more and more divisible by p, this is just the interpretation of what it means to be close with respect to the p-adic absolute value. The writing of α_n and α_m in base p will thus be the same for more and more terms starting from the beginning, so that (α_n) defines a p-adic number.

This may get clearer if one tries to write down two p-adic numbers. If a, b are p-adic integers, $a = a_0 + a_1 p + a_2 p^2 + \ldots$, $b = b_0 + b_1 p + b_2 p^2 + \ldots$, if $a_0 \neq b_0$, then $|a - b|_p = p^0 = 1$ if p does not divide $a_0 - b_0$, and $|a - b|_p = p^{-1}$ if $p | a_0 - b_0$, but $|a - b|_p$ cannot be smaller than $1/p$, for which we need $a_0 = b_0$. This works similarly for a, b p-adic numbers. Then we can write $a = a_{-k}1/p^k + \ldots$, $b = b_{-l}1/p^l + \ldots$. If $k \neq l$, say $k > l$, then $|a - b|_p = |b_{-l}1/p^l + \ldots + a_{-k}/p^k + \ldots|_p = p^l$, which is positive. The two p-adic numbers a and b are thus very far apart. We see that for the distance between a and b to be smaller than 1, we first need all the coefficients a_{-i}, b_{-i}, to be the same, for $i = k, \ldots, 1$. We are then back to the computations we did for a and b p-adic integers.

We have just shown that

Theorem 5.3. *The field of p-adic numbers $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ with respect to the p-adic metric induced by $|\cdot|_p$.*

Now that we have a formal definition of the field of the p-adic numbers, let us look at some of its properties.

Proposition 5.4. *Let $\mathbb{Q}_p$ be the field of the p-adic numbers.*

1. *The unit ball $\{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\}$ is equal to $\mathbb{Z}_p$.*

2. *The p-adic units are*

$$\begin{aligned} \mathbb{Z}_p^\times &= \{\alpha \in \mathbb{Z}_p \mid 0 \neq a_0 \in (\mathbb{Z}/p\mathbb{Z})^\times\} \\ &= \{\alpha \in \mathbb{Z}_p \mid |\alpha|_p = 1\}. \end{aligned}$$

3. *The only non-zero ideals of $\mathbb{Z}_p$ are the principal ideals*

$$p^k\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid \mathrm{ord}_p(\alpha) \geq k\}.$$

4. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. 1. We look at the unit ball, that is $\alpha \in \mathbb{Q}_p$ such that $|\alpha|_p \leq 1$. By definition, we have

$$|\alpha|_p \leq 1 \iff p^{-\mathrm{ord}_p(\alpha)} \leq 1 \iff \mathrm{ord}_p(\alpha) \geq 0.$$

This is exactly saying that α belongs to $\mathbb{Z}_p$.

2. Let us now look at the units of $\mathbb{Z}_p$. Let α be a unit. Then

$$\alpha \in \mathbb{Z}_p^\times \iff \alpha \in \mathbb{Z}_p \text{ and } \frac{1}{\alpha} \in \mathbb{Z}_p \iff |\alpha|_p \leq 1 \text{ and } |1/\alpha|_p \leq 1 \iff |\alpha|_p = 1.$$

3. We are now interested in the ideals of $\mathbb{Z}_p$. Let I be a non-zero ideal of $\mathbb{Z}_p$, and let α be the element of I with minimal valuation $\mathrm{ord}_p(\alpha) = k \geq 0$. We thus have that

$$\alpha = p^k(a_k + a_{k+1}p + \ldots)$$

where the second factor is a unit, implying that

$$\alpha\mathbb{Z}_p = p^k\mathbb{Z}_p \subset I.$$

We now prove that $I \subset p^k\mathbb{Z}_p$, which concludes the proof by showing that $I = p^k\mathbb{Z}_p$. If I is not included in $p^k\mathbb{Z}_p$, then there is an element in I out of $p^k\mathbb{Z}_p$, but then this element must have a valuation smaller than k, which cannot be by minimality of k.

4. We now want to prove that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Formally, that means that for every element $\alpha \in \mathbb{Z}_p$, and every $\epsilon > 0$, we have $B(\alpha, \epsilon) \cap \mathbb{Z}$ is non-empty (where $B(\alpha, \epsilon)$ denotes an open ball around α of radius ϵ).

   Let us thus take $\alpha \in \mathbb{Z}_p$ and $\epsilon > 0$. There exists a k big enough so that $p^{-k} < \epsilon$. We set $\bar{\alpha} \in \mathbb{Z}$ the integer obtained by cutting the serie of α after $a_{k-1}p^{k-1}$. Then
   $$\alpha - \bar{\alpha} = a_k p^k + a_{k+1} p^{k+1} + \dots$$
   implies that
   $$|\alpha - \bar{\alpha}|_p \leq p^{-k} < \epsilon.$$
   Thus $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Similarly, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

□

The main definitions and results of this chapter are

- Definition of p-adic integers using p-adic expansions, inverse limit, and that they form a ring $\mathbb{Z}_p$
- Definition of p-adic numbers using p-adic expansions, and that they form a field $\mathbb{Q}_p$
- Definition of p-adic valuation and absolute value
- The product formula
- The formal definition of $\mathbb{Q}_p$ as completion of $\mathbb{Q}$, and that $\mathbb{Z}_p$ can then be defined as elements of $\mathbb{Q}_p$ with positive p-adic valuation.
- Ideals and units of $\mathbb{Z}_p$.

Chapter 6

Valuations

In this chapter, we generalize the notion of absolute value. In particular, we will show how the p-adic absolute value defined in the previous chapter for $\mathbb{Q}$ can be extended to hold for number fields. We introduce the notion of archimedean and non-archimedean places, which we will show yield respectively infinite and finite places. We will characterize infinite and finite places for number fields, and show that they are very well known: infinite places correspond to the embeddings of the number field into $\mathbb{C}$ while finite places are given by prime ideals of the ring of integers.

6.1 Definitions

Let K be a field.

Definition 6.1. An absolute value on K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ which satisfies

- $|\alpha| = 0$ if and only if $\alpha = 0$,
- $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in K$
- there exists $a > 0$ such that $|\alpha + \beta|^a \leq |\alpha|^a + |\beta|^a$.

We suppose that the absolute value $|\cdot|$ is not trivial, that is, there exists $\alpha \in K$ with $|\alpha| \neq 0$ and $|\alpha| \neq 1$.

Note that when $a = 1$ in the last condition, we say that $|\cdot|$ satisfies the triangle inequality.

Example 6.1. The p-adic absolute valuation $|\cdot|_p$ of the previous chapter, defined by $|\alpha|_p = p^{-\mathrm{ord}_p(\alpha)}$ satisfies the triangle inequality.

Definition 6.2. Two absolute values are equivalent if there exists a $c > 0$ such that $|\alpha|_1 = (|\alpha|_2)^c$. An equivalence class of absolute value is called a place of K.

Example 6.2. Ostrowski's theorem, due to the mathematician Alexander Ostrowski, states that any non-trivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value ($|\cdot|$) or a p-adic absolute value ($|\cdot|_p$). Since $|\cdot| = |\cdot|_\infty$, we have that the places of $\mathbb{Q}$ are $|\cdot|_p$, $p \leq \infty$. By analogy we also call $p \leq \infty$ places of $\mathbb{Q}$.

Note that any valuation makes K into a metric space with metric given by $d(x_1, x_2) = |x_1 - x_2|^a$. This metric does depend on a, however the induced topology only depends on the place. This is what the above definition really means: two absolute values on a field K are equivalent if they define the same topology on K, or again in other words, that every set that is open with respect to one topology is also open with respect to the other (recall that by open set, we just mean that if an element belongs to the set, then it also belongs to an open ball that is contained in the open set).

Lemma 6.1. *Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on a field K. The following statements are equivalent:*

1. *$|\cdot|_1$ and $|\cdot|_2$ define the same topology;*
2. *for any $\alpha \in K$, we have $|\alpha|_1 < 1$ if and only if $|\alpha|_2 < 1$;*
3. *$|\cdot|_1$ and $|\cdot|_2$ are equivalent, that is, there exists a positive real $c > 0$ such that $|\alpha|_1 = (|\alpha|_2)^c$.*

Proof. We prove 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1.

(1. $\Rightarrow$ 2.) If $|\cdot|_1$ and $|\cdot|_2$ define the same topology, then any sequence that converges with respect to one absolute value must also converge in the other. But given any $\alpha \in K$, we have that

$$\lim_{n\to\infty} \alpha^n = 0 \iff \lim_{n\to\infty} |\alpha^n| = 0$$

with respect to the topology induced by an absolute value $|\cdot|$ (may it be $|\cdot|_1$ or $|\cdot|_2$) if and only if $|\alpha| < 1$. This gives 2.

(2. $\Rightarrow$ 3.) Since $|\cdot|_1$ is not trivial, there exists an element $x_0 \in K$ such that $|x_0|_1 < 1$. Let us set $c > 0$, $c \in \mathbb{R}$, such that

$$|x_0|_1^c = |x_0|_2.$$

We can always do that for a given x_0, the problem is now to see that this holds for any $x \in K$. Let $0 \neq x \in K$. We can assume that $|x|_1 < 1$ (otherwise just replace x by $1/x$). We now set $\lambda \in \mathbb{R}$ such that

$$|x|_1 = |x_0|_1^\lambda.$$

Again this is possible for given x and x_0. We can now combine that

$$|x|_1 = |x_0|_1^\lambda \Rightarrow |x|_1^c = |x_0|_1^{c\lambda}$$

with

$$|x_0|_1^c = |x_0|_2 \Rightarrow |x_0|_1^{c\lambda} = |x_0|_2^{\lambda}$$

to get that

$$|x|_1^c = |x_0|_1^{c\lambda} = |x_0|_2^{\lambda}.$$

We are left to connect $|x_0|_2^{\lambda}$ with $|x|_2$.

If $m/n > \lambda$, with $m, n \in \mathbb{Z}$, $n > 0$, then

$$\left|\frac{x_0^m}{x^n}\right|_1 = |x_0^{m-\lambda n}|_1 \left|\frac{x_0^{\lambda n}}{x^n}\right|_1 = |x_0|_1^{m-\lambda n} < 1.$$

Thus, by assumption from 2.,

$$\left|\frac{x_0^m}{x^n}\right|_2 < 1$$

that is

$$|x|_2 > |x_0|_2^{m/n} \text{ for all } \frac{m}{n} > \lambda,$$

or in other words,

$$|x|_2 > |x_0|_2^{\lambda+\beta},\ \beta > 0 \Rightarrow |x|_2 \geq |x_0|_2^{\lambda}.$$

Similarly, if $m/n < \lambda$, we get that $|x|_2 < |x_0|_2^{m/n} \Rightarrow |x|_2 \leq |x_0|_2^{\lambda}$. Thus

$$|x|_2 = |x_0|_2^{\lambda} = |x_0|_1^{c\lambda} = |x|_1^c$$

for all $x \in K$.

(3. $\Rightarrow$ 1.) If we assume 3., we get that

$$|\alpha - a|_1 < r \iff |\alpha - a|_2^c < r \iff |\alpha - a|_2 < r^{1/c},$$

so that any open ball with respect to $|\cdot|_1$ is also an open ball (albeit of different radius) with respect to $|\cdot|_2$. This is enough to show that the topologies defined by the two absolute values are identical. Note that having balls of different radius tells us that the metrics are different. □

6.2 Archimedean places

Let K be a number field.

Definition 6.3. An absolute value on a number field K is archimedean if for all $n > 1$, $n \in \mathbb{N}$, we have $|n| > 1$.

The story goes that since for an Archimedean valuation, we have $|m|$ tends to infinity with m, the terminology recalls the book that Archimedes wrote, called "On Large Numbers".

Proposition 6.2. *The only archimedean place of $\mathbb{Q}$ is the place of the real absolute value $|\cdot|_\infty$.*

Proof. Let $|\cdot|$ be an archimedean absolute value on $\mathbb{Q}$. We can assume that the triangle inequality holds (otherwise, we replace $|\cdot|$ by $|\cdot|^a$). We have to prove that there exists a constant $c > 0$ such that $|x| = |x|_\infty^c$ for all $x \in \mathbb{Q}$. Let us first start by proving that this is true for positive integers.

Let $m, n > 1$ be integers. We write m in base n:

$$m = a_0 + a_1 n + a_2 n^2 + \ldots + a_r n^r,\ 0 \leq a_i < n.$$

In particular, $m \geq n^r$, and thus

$$r \leq \frac{\log m}{\log n}.$$

Thus, we can upper bound $|m|$ as follows:

$$\begin{aligned} |m| &\leq |a_0| + |a_1||n| + \ldots + |a_r||n|^r \\ &\leq (|a_0| + |a_1| + \ldots + |a_r|)|n|^r \text{ since } |n| > 1 \\ &\leq (1+r)|n|^{r+1} \\ &\leq \left(1 + \frac{\log m}{\log n}\right) |n|^{\frac{\log m}{\log n}+1}. \end{aligned}$$

Note that the second inequality is not true for example for the p-adic absolute value! We can do similarly for m^k, noticing that the last term is of order at most n^{rk}. Thus

$$|m|^k \leq \left(1 + \frac{k \log m}{\log n}\right) |n|^{\frac{k \log m}{\log n}+1},$$

and

$$|m| \leq \left(1 + \frac{k \log m}{\log n}\right)^{1/k} |n|^{\frac{\log m}{\log n}+1/k}.$$

If we take the limit when $k \to \infty$ (recall that $\sqrt[n]{n} \to 1$ when $n \to \infty$), we find that

$$|m| \leq |n|^{\frac{\log m}{\log n}}.$$

If we exchange the role of m and n, we find that

$$|n| \leq |m|^{\frac{\log n}{\log m}}.$$

Thus combining the two above inequalities, we conclude that

$$|n|^{1/\log n} = |m|^{1/\log m}$$

which is a constant, say e^c. We can then write that

$$|m| = e^{c \log m} = m^c = |m|_\infty^c$$

since $m > 1$. We have thus found a suitable constant $c > 0$, which concludes the proof when m is a positive integer.

To complete the proof, we notice that the absolute value can be extended to positive rational number, since $|a/b| = |a|/|b|$, which shows that $|x| = |x|_\infty^c$ for $0 < x \in \mathbb{Q}$. Finally, it can be extended to arbitrary elements in $\mathbb{Q}$ by noting that $|-1| = 1$. □

Let K be a number field and $\sigma : K \to \mathbb{C}$ be an embedding of K into $\mathbb{C}$, then $|x|_\sigma = |\sigma(x)|$ is an archimedean absolute value.

Theorem 6.3. *Let K be a number field. Then there is a bijection*

$$\{ \text{ archimedean places } \} \leftrightarrow \{ \text{ embeddings of } K \text{ into } \mathbb{C} \text{ up to conjugation } \}.$$

The archimedean places are also called places at infinity. We say that $|\cdot|$ is a real place if it corresponds to a real embedding. A pair of complex conjugate embeddings is a complex place.

6.3 Non-archimedean places

Let K be a number field. By definition, an absolute value: $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is non-archimedean if there exists $n > 1$, $n \in \mathbb{N}$, such that $|n| < 1$.

Lemma 6.4. *For a non-archimedean absolute value on $\mathbb{Q}$, we have that*

$$|m| \leq 1, \text{ for all } m \in \mathbb{Z}.$$

Proof. We can assume that $|\cdot|$ satisfies the triangle inequality. Let us assume by contradiction that there exists $m \in \mathbb{Z}$ such that $|m| > 1$. There exists $M = m^k$ such that

$$|M| = |m|^k > \frac{n}{1 - |n|},$$

where n is such that $|n| < 1$, which exists by definition. Let us now write M in base n:

$$M = a_0 + a_1 n + \ldots + a_r n^r$$

which is such that

$$\begin{aligned} |M| &\leq |a_0| + |a_1||n| + \ldots + |a_r||n|^r \\ &< n(1 + |n| + \ldots + |n|^r) \end{aligned}$$

since $|a_i| = |1 + \ldots + 1| \leq a_i|1| < n$. Thus

$$|M| < n \sum_{j \geq 0} |n|^j = \frac{n}{1 - |n|}$$

which is a contradiction. □

Lemma 6.5. *Let $|\cdot|$ be a non-archimedean absolute value which satisfies the triangle inequality. Then*

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

for all $\alpha, \beta \in K$. We call $|\cdot|$ ultrametric.

Proof. Let $k > 0$. We have that

$$\begin{aligned} |\alpha+\beta|^k &= |(\alpha+\beta)^k| \\ &= \left|\sum_{j=0}^{k}\binom{k}{j}\alpha^j\beta^{k-j}\right| \\ &\leq \sum_{j=0}^{k}\left|\binom{k}{j}\right||\alpha|^j|\beta|^{k-j}. \end{aligned}$$

By the previous lemma, we have that $\left|\binom{k}{j}\right| \leq 1$, so that

$$|\alpha+\beta|^k \leq (k+1)\max\{|\alpha|,|\beta|\}^k.$$

Thus

$$|\alpha+\beta| \leq \sqrt[k]{k+1}\max\{|\alpha|,|\beta|\}.$$

We get the result by observing $k \to \infty$. □

Proposition 6.6. *let K be a number field, and $|\cdot|$ be a non-archimedean absolute value. Let $\alpha \neq 0$. Then there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and a constant $C > 1$ such that*

$$|\alpha| = C^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)},$$

where $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ is the highest power of $\mathfrak{p}$ which divides $\alpha\mathcal{O}_K$.

Definition 6.4. We call

$$\mathrm{ord}_{\mathfrak{p}} : K^\times \to \mathbb{Z}$$

the $\mathfrak{p}$-adic valuation.

Proof. We can assume that $|\cdot|$ satisfies the triangle inequality. It is enough to show the formula for $\alpha \in \mathcal{O}_K$.

We already know that $|m| \leq 1$ for all $m \in \mathbb{Z}$. We now extend this result for elements of $\mathcal{O}_K$.

($|\alpha| \leq 1$ for $\alpha \in \mathcal{O}_K$). For $\alpha \in \mathcal{O}_K$, we have an equation of the form

$$\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0 = 0,\ a_i \in \mathbb{Z}.$$

Let us assume by contradiction that $|\alpha| > 1$. By Lemma 6.4, we have that $|a_i| \leq 1$ for all i. In the above equation, the term α^m is thus the one with maximal absolute value. By Lemma 6.5, we get

$$\begin{aligned} |\alpha|^m &= |a_{m-1}\alpha^{m-1} + \ldots + a_0| \\ &\leq \max\{|a_{m-1}||\alpha|^{m-1}, \ldots, |a_1||\alpha|, |a_0|\} \\ &\leq \max\{|\alpha|^{m-1}, \ldots, 1\} \end{aligned}$$

thus a contradiction. We have thus shown that $|\alpha| \leq 1$ for all $\alpha \in \mathcal{O}_K$. We now set

$$\mathfrak{p} = \{\alpha \in \mathcal{O}_K \mid |\alpha| < 1\}.$$

($\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.) Let us first show that $\mathfrak{p}$ is an ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{p}$ and $\beta \in \mathcal{O}_K$. We have that

$$|\alpha\beta| = |\alpha||\beta| \leq |\alpha| < 1$$

showing that $\alpha\beta \in \mathfrak{p}$ and $\alpha + \beta \in \mathfrak{p}$ since

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

where the first inequality follows from Lemma 6.5. Let us now show that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. If $\alpha, \beta \in \mathcal{O}_K$ are such that $\alpha\beta \in \mathfrak{p}$, then $|\alpha||\beta| < 1$, which means that at least one of the two terms has to be < 1, and thus either α or β are in $\mathfrak{p}$.

(There exists a suitable $C > 1$.) We now choose π in $\mathfrak{p}$ but not in $\mathfrak{p}^2$ and let α be an element of $\mathcal{O}_K$. We set $m = \mathrm{ord}_{\mathfrak{p}}(\alpha)$. We consider α/π^m, which is of valuation 0 (by choice of π and m). We can write

$$\frac{\alpha}{\pi^m}\mathcal{O}_K = IJ^{-1}$$

with I and J are integral ideals, both prime to $\mathfrak{p}$. By the Chinese Remainder Theorem, there exists $\beta \in \mathcal{O}_K$, $\beta \in J$ and β prime to $\mathfrak{p}$. We furthermore set

$$\gamma = \beta\frac{\alpha}{\pi^m} \in I \subset \mathcal{O}_K.$$

Since both γ and β are elements of $\mathcal{O}_K$ not in $\mathfrak{p}$, we have that $|\gamma| = 1$ and $|\beta| = 1$ (if this is not clear, recall the definition of $\mathfrak{p}$ above). Thus

$$\left|\frac{\alpha}{\pi^m}\right| = \left|\frac{\gamma}{\beta}\right| = 1.$$

We have finally obtained that

$$|\alpha| = |\pi|^m$$

for all $\alpha \in \mathcal{O}_K$, so that we conclude by setting

$$C = \frac{1}{|\pi|}.$$

□

Corollary 6.7. *For a number field K, we have the following bijection*

$$\{\textit{places of } K\} \leftrightarrow \{\textit{real embeddings}\} \cup \{\textit{pairs of complex embeddings}\} \cup \{\textit{prime ideals}\}.$$

For each place of a number field, there exists a canonical choice of absolute values (called normalized absolute values).

- real places:
$$|\alpha| = |\sigma(\alpha)|_{\mathbb{R}},$$
where σ is the associated embedding.

- complex places:
$$|\alpha| = |\sigma(\alpha)|_{\mathbb{C}}^2 = |\sigma(\alpha)\bar{\sigma}(\alpha)|_{\mathbb{R}},$$
where $(\sigma, \bar{\sigma})$ is the pair of associated complex embeddings.
- finite places (or non-archimedean places):
$$|\alpha| = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}$$
where $\mathfrak{p}$ is the prime ideal associated to $|\cdot|$.

Proposition 6.8. (Product Formula). *For all $0 \neq \alpha \in K$, we have*
$$\prod_{\nu} |\alpha|_\nu = 1$$
where the product is over all places ν, and all the absolute values are normalized.

Proof. Let us rewrite the product as
$$\prod_{\nu} |\alpha|_\nu = \prod_{\nu \text{ finite}} |\alpha|_\nu \prod_{\nu \text{ infinite}} |\alpha|_\nu$$
We now compute $\mathrm{N}(\alpha\mathcal{O}_K)$ in two ways, one which will make appear the finite places, and the other the infinite places. First,
$$\mathrm{N}(\alpha\mathcal{O}_K) = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(\alpha)} = \prod_{\nu \text{ finite}} |\alpha|_\nu^{-1}$$
which can be alternatively computed by
$$\mathrm{N}(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|_{\mathbb{R}} = \prod_{\sigma} |\sigma(\alpha)|_{\mathbb{C}} = \prod_{\nu \text{ infinite}} |\alpha|_\nu.$$
□

6.4 Weak approximation

We conclude this chapter by proving the weak approximation theorem. The term "weak" can be thought by opposition to the "strong approximation theorem", where in the latter, we will state the existence of an element in $\mathcal{O}_K$, while we are only able to guarantee this element to exist in K for the former. Those approximation theorems (especially the strong one) restate the Chinese Remainder Theorem in the language of valuations.

Let K be a number field.

Lemma 6.9. *Let ω be a place of K and $\{\nu_1, \ldots, \nu_N\}$ be places different from ω. Then there exists $\beta \in K$ such that $|\beta|_\omega > 1$ and $|\beta|_{\nu_i} < 1$ for all $i = 1, \ldots, N$.*

Proof. We do a proof by induction on N.

(N=1). Since $|\cdot|_{\nu_1}$ is different from $|\cdot|_\omega$, they induce different topologies, and thus there exists $\delta \in K$ with

$$|\delta|_{\nu_1} < 1 \text{ and } |\delta|_\omega \geq 1$$

(recall that we proved above that if the two induced topologies are the same, then $|\delta|_{\nu_1}| < 1$ implies $|\delta|_\omega| < 1$). Similarly, there exists $\gamma \in K$ with

$$|\gamma|_\omega < 1 \text{ and } |\gamma|_{\nu_1} \geq 1.$$

We thus take $\beta = \delta\gamma^{-1}$.

(Assume true for $N-1$). We assume $N \geq 2$. By induction hypothesis, there exists $\gamma \in K$ with

$$|\gamma|_\omega > 1 \text{ and } |\gamma|_{\nu_i} < 1,\ i = 1, \ldots, N-1.$$

Again, as we proved in the case $N = 1$, we can find δ with

$$|\delta|_\omega > 1 \text{ and } |\delta|_{\nu_N} < 1.$$

We have now 3 cases:

- if $|\gamma|_{\nu_N} < 1$: then take $\beta = \gamma$. We have that $|\beta|_\omega > 1$, $|\beta|_{\nu_i} < 1$, $i = 1, \ldots, N-1$ and $|\beta|_{\nu_N} < 1$.
- if $|\gamma|_{\nu_N} = 1$: we have that $\gamma^r \to 0$ in the ν_i-adic topology, for all $i < N$. There exists thus $r >> 0$ such that

  $$\beta = \gamma^r \delta$$

  which satisfies the required inequalities. Note that $|\beta|_\omega > 1$ and $|\beta|_{\nu_N} > 1$ are immediately satisfied, the problem is for ν_i, $i = 1, \ldots, N-1$ where we have no control on $|\delta|_{\nu_i}$ and need to pick $r >> 0$ to satisfy the inequality.
- if $|\gamma|_{\nu_N} > 1$: we then have that

  $$\frac{\gamma^r}{1+\gamma^r} = \frac{1}{1+\frac{1}{\gamma^r}} \to_{r\to\infty} \begin{cases} 1 & \text{for } |\cdot|_{\nu_N} \\ 0 & \text{for } |\cdot|_{\nu_i},\ i < N \end{cases}$$

  Take

  $$\beta = \frac{\gamma^r}{1+\gamma^r}\delta,\ r >> 0.$$

□

Theorem 6.10. *Let K be a number field, $\epsilon > 0$, $\{\nu_1, \ldots, \nu_m\}$ be distinct places of K, and $\alpha_1, \ldots, \alpha_m \in K$. Then there exist $\beta \in K$ such that*

$$|\beta - \alpha_i|_{\nu_i} < \epsilon.$$

Proof. By the above lemma, there exist $\beta_j \in K$ with $|\beta_j|_{\nu_j} > 1$ and $|\beta_j|_{\nu_i} < 1$ for $i \neq j$. Set

$$\gamma_r = \sum_{j=1}^{m} \frac{\beta_j^r}{1+\beta_j^r}\alpha_j.$$

When $r \to \infty$, we have $\gamma_r \to \alpha_j$ for the ν_j-adic topology, since as in the above proof

$$\frac{\beta^r}{1+\beta^r} = \frac{1}{1+\frac{1}{\beta^r}} \to_{r\to\infty} \begin{cases} 1 & \text{for } |\beta_j|_{\nu_j} > 1 \\ 0 & \text{for } |\beta_j|_{\nu_i} < 1,\ i \neq j. \end{cases}$$

Thus take $\beta = \gamma_r$, $r >> 0$. □

Let K_{ν_i} be the completion of K with respect to the ν_i-adic topology. We can restate the theorem by saying that the image of

$$K \to \prod_{i=1}^{m} K_{\nu_i},\ x \mapsto (x, x, \ldots, x)$$

is dense.

The main definitions and results of this chapter are

- Definition of absolute value, of place, of archimedean and non-archimedean places
- What are the finite/infinite places for number fields
- The product formula

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.

Bibliography

[1] H. Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields*. Springer-Verlag, NY, 1978.

[2] A. Fröhlich and M.J. Taylor. *Algebraic number theory*. Cambridge University Press, Great Britain, 1991.

[3] F.Q. Gouvea. *p-adic Numbers: An Introduction*. Springer Verlag, 1993.

[4] G. Gras. *Class Field Theory*. Springer Verlag, 2003.

[5] P. Samuel. *Théorie algébrique des nombres*. Hermann, 1971.

[6] I.N. Stewart and D.O. Tall. *Algebraic Number Theory*. Chapman and Hall, 1979.

[7] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. University Press of Cambridge, 2001.