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 $0 \le a_i \le p - 1$.

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:

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

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

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

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

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

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 $\alpha = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \ldots$ 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

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

By iterating the above computations, we get that

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

The other solution is given by

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

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:

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

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

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

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 $\text{ord}_p(a-b)$ 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

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

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

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

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

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

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

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, $a = a_0 + a_1 p + a_2 p^2 + \dots$, $b = b_0 + b_1 p + b_2 p^2 + \dots$, 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 $a = a_{-k}1/p^k + \dots$, $b = b_{-l}1/p^l + \dots$. If $k \neq l$, say $k > l$, then $|a - b|_p = |b_{-l}1/p^l + \dots + a_{-k}/p^k + \dots|_p = p^l$, 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 $i = k, \dots, 1$. 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*

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

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

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

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 $\operatorname{ord}_p(\alpha) = k \geq 0$. 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 $\mathbb{Z}_p$.