1. Why local fields?

When attempting to determine whether a Diophantine equation has solutions over the integers, it is only natural to consider first whether it has solutions modulo \( p \) for different \( p \). Similarly, when we try to analyze rings of integers, we frequently benefit from analyzing one prime at a time by considering the local rings. The theory of local fields may be viewed as lying between these two approaches: we will obtain more information than we would just working modulo \( p \), but not as much as working in the local ring of the ring of integers itself. Conversely, while the structure of local fields is more complex than that of finite fields, it is simpler, or at least easier to analyze, than the structure of the number fields themselves.

The tool for achieving this is completion. Just as \( \mathbb{R} \) is the completion of \( \mathbb{Q} \) with respect to the standard absolute value, and it is easier to analyze roots of polynomials and algebraic extensions in \( \mathbb{R} \) than in \( \mathbb{Q} \), local fields will be completions of number fields with respect to \( p \)-adic absolute values, and it is easier to analyze roots of polynomials and algebraic extensions in the local field case.

2. The \( p \)-adic integers

We describe three constructions of \( \mathbb{Z}_p \), the \( p \)-adic integers, and see that they are equivalent. We fix a prime number \( p \) for the remainder of the discussion.

**Definition 2.1.** The ring \( \mathbb{Z}_p \) is defined to be the set of integers written in base \( p \), and allowed to have infinitely many digits, under the addition and multiplication obtained by the usual formulas.

Since the usual laws for addition and multiplication give formulas for the \( n \)th digit in terms of previous digits, we can use them just as well to add and multiply numbers with infinitely many digits.

**Definition 2.2.** The ring \( \mathbb{Z}_p \) is defined to be \( \{ (a_0, a_1, a_2, \ldots) : a_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}, a_{i+1} \equiv a_i \pmod{p^{i+1}} \} \), with coordinatewise addition and multiplication.

**Remark 2.3.** This is the same thing as saying that \( \mathbb{Z}_p \) is the inverse limit over the rings \( \mathbb{Z}/p^n\mathbb{Z} \) under the usual quotient maps.

The final definition requires some preliminary terminology.

**Definition 2.4.** We define the \( p \)-adic valuation \( \nu_p : \mathbb{Q}^* \to \mathbb{Z} \) by \( \nu_p(\frac{x}{y}) = \text{ord}_p(x) - \text{ord}_p(y) \). The \( p \)-adic absolute value \( || \cdot ||_p : \mathbb{Q} \to \mathbb{R}_{\geq 0} \) is defined by \( ||z||_p = p^{-\nu_p(z)} \) for \( z \neq 0 \), and \( ||0||_p = 0 \).

Thus, under the \( p \)-adic absolute value, the more powers of \( p \) that are in a number, the “smaller” it is.
Easy Facts 2.5. \( \nu_p \) satisfies:

(i) \( \nu_p(-1) = 0; \)
(ii) \( \nu_p(z_1 z_2) = \nu_p(z_1) + \nu_p(z_2); \)
(iii) \( \nu_p(z_1 + z_2) \geq \min\{\nu_p(z_1), \nu_p(z_2)\}. \)

\( || \cdot ||_p \) satisfies:

(i) \( ||z||_p = 0 \) if and only if \( z = 0; \)
(ii) \( ||-1||_p = 1; \)
(iii) \( ||z_1 z_2||_p = ||z_1||_p ||z_2||_p; \)
(iv) \( ||z_1 + z_2||_p \leq \max\{||z_1||_p, ||z_2||_p\}. \)

In particular, \( || \cdot ||_p \) satisfies the triangle inequality, and induces a metric on \( \mathbb{Q} \), and hence on \( \mathbb{Z} \).

Definition 2.6. The ring \( \mathbb{Z}_p \) is the completion of \( \mathbb{Z} \) with respect to the metric \( d(x, y) := ||x - y||_p. \)

Proposition 2.7. The three definitions of \( \mathbb{Z}_p \) above are equivalent.

Proof. It is easy to see that the first two definitions are the same: indeed, an element of \( \mathbb{Z}/p^n \mathbb{Z} \) may be written uniquely as an integer base \( p \) with at most \( n \) digits, and the number obtained from this by taking the image in \( \mathbb{Z}/p^{n-1} \mathbb{Z} \) is simply obtained by dropping the highest digit. Thus we obtain a natural bijection.

To see that the second and third definitions agree, we note that sending \( a_i \in \mathbb{Z}/p^{i+1} \mathbb{Z} \) to any representative of it in \( \mathbb{Z} \) gives a Cauchy sequence under the metric \( d(\cdot, \cdot) \), and one checks that for different choices of representatives, we obtain Cauchy sequences whose differences tend to 0, and are therefore equivalent in the completion, so we obtain a well-defined map from the second set to the third. We obtain a map back via the observation that if \((b_0, b_1, b_2, \ldots)\) is a Cauchy sequence of integers, then for any \( i \), there exists \( N \) such that for all \( n_1, n_2 \geq N \), \( b_{n_1} \equiv b_{n_2} \pmod{p^{i+1}} \). We can then set \( a_i = b_N \), and doing this for each \( i \) gives a map from the third set to the second. It is easy to check that these maps are mutually inverse, and hence define a bijection.

Since the addition and multiplication in all definitions are obtained from that of the integers, it is easy to see that they agree. \( \square \)

Under the second definition of \( \mathbb{Z}_p \), it is easy to check that it is an integral domain, since if two elements are non-zero in the \( i \)th and \( j \)th places respectively, their product must be non-zero in the \((i + j)\)th place. We can then define \( \mathbb{Q}_p \) to be the field of fractions of \( \mathbb{Z}_p \).

At this point, it seems reasonable to wonder what makes \( \mathbb{Z}_p \) simpler in any sense that the local ring \( \mathbb{Z}_{(p)} \subset \mathbb{Q} \). One answer is provided by the following, which is elementary to prove, and which we will give a stronger version of next time:

Lemma 2.8. (Hensel’s) Suppose that \( f(x) \in \mathbb{Z}[x] \) is such that there exists an \( x_0 \in \mathbb{Z} \) with \( f(x_0) \equiv 0 \pmod{p} \), and \( f'(x_0) \not\equiv 0 \pmod{p} \). Then there exists a root of \( f(x) \) in \( \mathbb{Z}_p \) agreeing with \( x_0 \) modulo \( p \).

3. The general case

Let \( K \) be a number field, and \( p \) a prime ideal of \( \mathcal{O}_K \). Recall that for \( x \in K^* \), we had defined \( \text{ord}_p(x) \) to be the number of powers of \( p \) (possibly negative) occurring in
the prime factorization of the fractional ideal \( x\mathcal{O}_K \). In keeping with the preceding, we shall write \( \nu_p(x) := \text{ord}_p(x) \).

**Definition 3.1.** We define the \( p \)-adic absolute value \( || \cdot ||_p : K \to \mathbb{R}_{\geq 0} \) by
\[
||x||_p = N(p)^{-\nu_p(x)} \quad \text{for} \quad x \neq 0, \quad \text{and} \quad ||0||_p = 0.
\]

**Easy Facts 3.2.** \( || \cdot ||_p \) satisfies:
(i) \( ||x||_p = 0 \) if and only if \( x = 0 \);
(ii) \( ||-1||_p = 1 \);
(iii) \( ||x_1x_2||_p = ||x_1||_p||x_2||_p \);
(iv) \( ||x_1 + x_2||_p \leq \max\{||x_1||_p, ||x_2||_p\} \).

Thus, as before, we get a metric \( d(x_1, x_2) := ||x_1 - x_2||_p \), and we can define:

**Definition 3.3.** \( K_p \) is the completion of \( K \) with respect to the metric \( d(\cdot, \cdot) \). \( \hat{\mathcal{O}}_{K,p} \) is the completion of \( \mathcal{O}_{K,p} \) with respect to the same metric.

The notation \( \hat{\mathcal{O}}_{K,p} \) is somewhat cumbersome, but we have already defined \( \mathcal{O}_{K,p} \) to be the standard local ring, and this notation is consistent with the standard notation of algebraic geometry.

**Proposition 3.4.** We have:
(i) \( K_p \) is the field of fractions of \( \hat{\mathcal{O}}_{K,p} \).
(ii) \( \hat{\mathcal{O}}_{K,p} \) is the subset of elements of \( K_p \) with absolute value at most 1.
(iii) \( \hat{\mathcal{O}}_{K,p} \) is also the completion of \( \mathcal{O}_{K,p} \) with respect to the metric \( d(\cdot, \cdot) \).
(iv) \( \hat{\mathcal{O}}_{K,p} \) is the inverse limit of \( \mathcal{O}_{K,p}/\mathfrak{p}^n \) as \( n \) varies.

We will prove this next time.