8.1 Completions of $\mathbb{Q}$

We already know that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to its archimedean absolute value $|\ |_\infty$. Now we consider the completion of $\mathbb{Q}$ with respect to any of its nonarchimedean absolute values $|\ |_p$.

Theorem 8.1. *The completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ with respect to the p-adic absolute value $|\ |_p$ is isomorphic to $\mathbb{Q}_p$. More precisely, there is an isomorphism $\pi\colon \mathbb{Q}_p \to \hat{\mathbb{Q}}$ that satisifies $|\pi(x)|_p = |x|_p$ for all $x \in \hat{\mathbb{Q}}$.*

Proof. For any $x \in \mathbb{Q}_p$ either $x \in \mathbb{Z}_p$ or $x^{-1} \in \mathbb{Z}_p$, since $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\}$, so to define π it is enough to give a ring homomorphism from $\mathbb{Z}_p$ to $\hat{\mathbb{Q}}$. Let us uniquely represent each $a \in \mathbb{Z}_p$ as a sequence of integers (a_n) with $a_n \in [0, p^n - 1]$, such that $a_{n+1} \equiv a_n \bmod \mathbb{Z}/p^n\mathbb{Z}$. For any $\epsilon > 0$ there is an integer N such that $p^{-N} < \epsilon$, and we then have $|a_m - a_n|_p < \epsilon$ for all $m, n \ge N$. Thus each $a \in \mathbb{Z}_p$ corresponds to a sequence of integers (a_n) that is Cauchy with respect to the p-adic absolute value on $\mathbb{Q}$ and we define $\pi(a)$ to be the equivalence class of (a_n) in $\hat{\mathbb{Q}}$. It follows immediately from the definition of addition and multiplication in both $\mathbb{Z}_p$ and $\hat{\mathbb{Q}}$ as element-wise operations on representative sequences that π is a ring homomorphism from $\mathbb{Z}_p$ to $\hat{\mathbb{Q}}$. Moreover, π preserves the absolute value $|\ |_p$, since

$$|a|_p = \lim_{n\to\infty} |a_n|_p = |\pi(a)|_p.$$

Here the first equality follows from the fact that if $v_p(a) = m$, then $a_n = 0$ for $n \le m$ and $v_p(a_n) = m$ for all $n > m$ (so the sequence $|a_n|_p$ eventually constant), and the second equality is the definition of $|\ |_p$ on $\hat{\mathbb{Q}}$.

We now extend π from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ by defining $\pi(x^{-1}) = \pi(x)^{-1}$ for all $x \in \mathbb{Z}_p$ (this is necessarily consistent with our definition of π on $\mathbb{Z}_p^\times$, since π is a ring homomorphism). As a ring homomorphism of fields, $\pi\colon \mathbb{Q}_p \to \hat{\mathbb{Q}}$ must be injective, so we have an embedding of $\mathbb{Q}_p$ into $\hat{\mathbb{Q}}$. To show this it is an isomorphism, it suffices to show that $\mathbb{Q}_p$ is complete, since then we can embed $\hat{\mathbb{Q}}$ into $\mathbb{Q}_p$, by Corollary 7.17.

So let (x_n) be a Cauchy sequence in $\mathbb{Q}_p$. Then (x_n) is bounded (fix $\epsilon > 0$, pick N so that $|x_n - x_N|_p < \epsilon$ for all $n \ge N$ and note that $|x_n|_p \le \max_{n\le N}(|x_n|_p) + \epsilon$). Thus for some fixed power p^r of p the sequence $(y_n) = (p^r x_n)$ lies in $\mathbb{Z}_p$. We now define $a \in \mathbb{Z}_p$ as a sequence of integers $(a_1, a_2, \ldots)$ with $a_i \in [0, p^i - 1]$ and $a_{i+1} \equiv a_i \bmod \mathbb{Z}/p^i\mathbb{Z}$ as follows. For each integer $i \ge 1$ pick N so that $|y_n - y_N| < p^{-i}$ for all $n \ge N$. Then $v_p(y_n - y_N) \ge i$, and we let a_i be the unique integer in $[0, p^i - 1]$ for which $y_n \equiv a_i \bmod \mathbb{Z}/p^i\mathbb{Z}$ for all $n \ge N$. We necessarily have $a_{i+1} \equiv a_i \bmod p^i$, so this defines an element a of $\mathbb{Z}_p$, and by construction (y_n) converges to a and therefore (x_n) converges to a/p^r. Thus every Cauchy sequence in $\mathbb{Q}_p$ converges, so $\mathbb{Q}_p$ is complete. ∎

It follows from Theorem 8.1 that we could have defined $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$, rather than as the fraction field of $\mathbb{Z}_p$, and many texts do exactly this. If we had taken this approach we would then define $\mathbb{Z}_p$ as the *the ring of integers* of $\mathbb{Q}_p$, that is, the ring

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\}.$$

Alternatively, we could define $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to $|\ |_p$.

Remark 8.2. The use of the term "ring of integers" in the context of a p-adic field can be slightly confusing. The ring $\mathbb{Z}_p$ is the *topological closure* of $\mathbb{Z}$ in $\mathbb{Q}_p$ (in other words, the completion of $\mathbb{Z}$), but it is not the *integral closure* of $\mathbb{Z}$ in $\mathbb{Q}_p$ (the elements in $\mathbb{Q}_p$ that are roots of a monic polynomial with coefficients in $\mathbb{Z}$). The latter set is countable, since there are only countably many polynomials with integer coefficients, but we know that $\mathbb{Z}_p$ is uncountable. But it is true that $\mathbb{Z}_p$ is integrally closed in $\mathbb{Q}_p$, every element of $\mathbb{Q}_p$ that is the root of a monic polynomial with coefficients in $\mathbb{Z}_p$ lies in $\mathbb{Z}_p$, so $\mathbb{Z}_p$ certainly contains the integral closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ (and is the completion of the integral closure).

8.2 Root-finding in p-adic fields

We now turn to the problem of finding roots of polynomials in $\mathbb{Z}_p[x]$. From Lecture 3 we already know how to find roots of polynomials in $(\mathbb{Z}/p\mathbb{Z})[x] \simeq \mathbb{F}_p[x]$. Our goal is to reduce the problem of root-finding over $\mathbb{Z}_p$ to root-finding over $\mathbb{F}_p$. To take the first step toward this goal we require the following compactness lemma.

Lemma 8.3. *Let (S_n) be an inverse system of finite non-empty sets with a compatible system of maps $f_n \colon S_{n+1} \to S_n$. The inverse limit $S = \varprojlim S_n$ is non-empty.*

Proof. If the f_n are all surjective, we can easily construct an element (s_n) of S: pick any $s_1 \in S_1$ and for $n \geq 1$ pick any $s_{n+1} \in f_n^{-1}(s_n)$. So our goal is to reduce to this case.

Let $T_{n,n} = S_n$ and for $m > n$, let $T_{m,n}$ be the image of S_m in S_n, that is

$$T_{m,n} = f_n(f_{n+1}(\cdots f_{m-1}(S_m) \cdots)).$$

For each n we then have an infinite sequence of inclusions

$$\cdots \subseteq T_{m,n} \subseteq T_{m-1,n} \subseteq \cdots \subseteq T_{n+1,n} \subseteq T_{n,n} = S_n.$$

The $T_{m,n}$ are all finite non-empty sets, and it follows that all but finitely many of these inclusions are equalities. Thus each infinite intersection $E_n = \bigcap_m T_{m,n}$ is a non-empty subset of S_n. Using the restriction of f_n to define a map $E_{n+1} \to E_n$, we obtain an inverse system (E_n) of finite non-empty sets whose maps are all surjective, as desired. $\square$

Theorem 8.4. *For any $f \in \mathbb{Z}_p[x]$ the following are equivalent:*

(a) *f has a root in $\mathbb{Z}_p$.*

(b) *$f \bmod p^n$ has a root in $\mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$.*

Proof. $(a) \Rightarrow (b)$: apply the projection maps $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ to the roots and coefficients of f. $(b) \Rightarrow (a)$: let S_n be the roots of f in $\mathbb{Z}/p^n\mathbb{Z}$ and consider the inverse system (S_n) of finite non-empty sets whose maps are the restrictions of the reduction maps from $\mathbb{Z}/p^{n+1}\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$. By Lemma 8.3, the set $S = \varprojlim S_n \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ is non-empty, and its elements are roots of f. $\square$

Theorem 8.4 reduces the problem of finding the roots of f in $\mathbb{Z}_p$ to the problem of finding roots of f modulo infinitely many powers of p. This might not seem like progress, but we will now show that under suitable conditions, once we have a root a_1 of $f \bmod p$, we can "lift" a_1 to a root a_n of $f \bmod p^n$, for each $n \geq 1$, and hence to a root of f in $\mathbb{Z}_p$.

A key tool in doing this is the Taylor expansion of f, which we now define in the general setting of a commutative ring R.[1]

[1] As always, our rings include a multiplicative identity 1.

Definition 8.5. Let $f \in R[x]$ be a polynomial of degree at most d and let $a \in R$. The (degree d) *Taylor expansion* of f about a is

$$f(x) = f_d(x-a)^d + f_{d-1}(x-a)^{d-1} + \cdots + f_1(x-a) + f_0,$$

with $f_0, f_1, \ldots, f_d \in R$.

The Taylor coefficients $f_0, f_1, \ldots, f_d$ are uniquely determined by the expansion of $f(y+z)$ in $R[y,z]$:

$$f(y+z) = f_d(y)z^d + f_{d-1}(y)z^{d-1} + \cdots + f_1(y)z + f_0(y).$$

Replacing y with a and z with $x-a$ yields the Taylor expansion of f with $f_i = f_i(a) \in R$.

This definition of the Taylor expansion agrees with the usual definition over $\mathbb{R}$ or $\mathbb{C}$ in terms of the derivatives of f.

Definition 8.6. Let $f(x) = \sum_{n=0}^{d} a_n x^n$ be a polynomial in $R[x]$. The *formal derivative* f' of f is the polynomial $f'(x) = \sum_{n=1}^{d} n a_n x^{n-1}$ in $R[x]$.

It is easy to check that the formal derivative satisfies the usual properties

$$\begin{aligned}(f+g)' &= f' + g',\\ (fg)' &= f'g + fg',\\ (f \circ g)' &= (f' \circ g)g'.\end{aligned}$$

Over a field of characteristic zero one then has the more familiar form of the Taylor expansion

$$f(x) = \frac{f^{(d)}(a)}{d!}(x-a)^d + \cdots + \frac{f^{(2)}(a)}{2}(x-a)^2 + f'(a)(x-a) + f(a),$$

where $f^{(n)}$ denotes the result of taking n successive derivatives ($f^{(n)}(a)$ is necessarily divisible by $n!$, so the coefficients lie in R). Regardless of the characteristic, the Taylor coefficients f_0 and f_1 always satisfy $f_0 = f(a)$ and $f_1 = f'(a)$.

Lemma 8.7. *Let $a \in R$ and $f \in R[x]$. Then $f(a) = f'(a) = 0$ if and only if a is (at least) a double root of f, that is, $f(x) = (x-a)^2 g(x)$ for some $g \in R[x]$.*

Proof. The reverse implication is clear: if $f(x) = (x-a)^2 g(x)$ then clearly $f(a) = 0$, and we have $f'(x) = 2(x-a)g(x) + (x-a)^2 g'(x)$, so $f'(a) = 0$ as well. For the forward implication, let $d = \max(\deg f, 2)$ and consider the degree d Taylor expansion of f about a:

$$f(x) = f_d(x-a)^d + f_{d-1}(x-a)^{d-1} + \cdots + f_2(x-a)^2 + f_1(x)(x-a) + f_0.$$

If $f(a) = f'(a) = 0$ then $f_0 = f(a) = 0$ and $f_1 = f'(a) = 0$ and we can put

$$f(x) = (x-a)^2 \left(f_d(x-a)^{d-2} + f_{d-2}(x-a)^{d-3} + \cdots + f_2 \right),$$

in the desired form. $\square$

8.3 Hensel's lemma

We are now ready to prove Hensel's lemma, which allows us to lift any simple root of $f \bmod p$ to a root of f in $\mathbb{Z}_p$.

Theorem 8.8 (Hensel's lemma)**.** *Let $a \in \mathbb{Z}_p$ and $f \in \mathbb{Z}_p[x]$. Suppose $f(a) \equiv 0 \bmod p$ and $f'(a) \not\equiv 0 \bmod p$. Then there is a unique $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $b \equiv a \bmod p$.*

Our strategy for proving Hensel's lemma is to apply Newton's method, regarding a as an approximate root of f that we can iteratively improve. Remarkably, unlike the situation over an archimedean field like $\mathbb{R}$ or $\mathbb{C}$, this is guaranteed to always work.

Proof. Let $a_1 = a$, and for $n \geq 1$ define

$$a_{n+1} = a_n - f(a_n)/f'(a_n).$$

We will prove by induction on n that the following hold

$$f'(a_n) \not\equiv 0 \bmod p, \tag{1}$$

$$f(a_n) \equiv 0 \bmod p^n, \tag{2}$$

Note that (1) ensures that $f'(a_n) \in \mathbb{Z}_p^\times$, so a_{n+1} is well defined and an element of $\mathbb{Z}_p$. Together with the definition of a_{n+1}, (1) and (2) imply $a_{n+1} \equiv a_n \bmod p^n$, which means that the sequence $(a_n \bmod p^n)$ defines an element of $b \in \mathbb{Z}_p$ for which $f(b) = 0$ and $b \equiv a_1 \equiv a$ modulo p (equivalently, the sequence (a_n) is a Cauchy sequence in $\mathbb{Z}_p$ with limit b).

The base case $n = 1$ is clear, so assume (1) and (2) hold for a_n. Then $a_{n+1} \equiv a_n \bmod p^n$, so $f'(a_{n+1}) \equiv f'(a_n) \bmod p^n$. Reducing mod p gives $f'(a_{n+1}) \equiv f'(a_n) \not\equiv 0 \bmod p$. So (1) holds for a_{n+1}. To show (2), let $d = \max(\deg f, 2)$ and consider the Taylor expansion of f about a_n:

$$f(x) = f_d(x - a_n)^d + f_{d-1}(x - a_n)^{d-1} + \cdots + f_1(x - a_n) + f_0.$$

Reversing the order of the terms and noting that $f_0 = f(a_n)$ and $f_1 = f'(a_n)$ we can write

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + (x - a_n)^2 g(x),$$

for some $g \in \mathbb{Z}_p[x]$. Substituting a_{n+1} for x yields

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2 g(a_{n+1}).$$

From the definition of a_{n+1} we have $f'(a_n)(a_{n+1} - a_n) = -f(a_n)$, thus

$$f(a_{n+1}) = (a_{n+1} - a_n)^2 g(a_{n+1}).$$

As noted above, $a_{n+1} \equiv a_n \bmod p^n$, so $f(a_{n+1}) \equiv 0 \bmod p^{2n}$. Since $2n \geq n + 1$, we have $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$, so (2) holds for a_{n+1}.

For uniqueness we argue that each a_{n+1} (and therefore b) is congruent modulo p^{n+1} to the *unique* root of $f \bmod p^{n+1}$ that is congruent to $a_n \bmod p^n$. There can be only one such root because a_n is a *simple* root of $f \bmod p^n$, since (1) implies $f'(a_n) \not\equiv 0 \bmod p^n$. $\square$

There are stronger version of Hensel's lemma than we have given here. In particular, the hypothesis $f'(a) \not\equiv 0 \bmod p$ can be weakened so that the lemma can be applied even in situations where a is not a simple root. Additionally, the sequence (a_n) actualy converges to a root of f more rapidly than indicated by inductive hypothesis (2). You will prove stronger and more effective versions of Hensel's lemma on the problem set, as well as exploring several applications.