Chapter 6 : p-adic numbers

No more number fields! Let us now study a different area of algebraic number theory, introduced by Kurt Hensel in an attempt to exploit the power of power series expansions in connection with numbers. While trying to explain the properties of (rational) integers mathematicians started embedding $\mathbb{Z}$ in bigger and bigger structures – richer and richer in properties. $\mathbb{Q}$ came in a natural attempt to form quotients, and for some time people believed that that's all about *real*ity. Pythagoras was seemingly the first to locate and prove the irrationality of a number, namely $\sqrt{2}$. It took mankind centuries for completing the picture of the *real line*. One possibility is to look $\mathbb{R}$ as the *completion* of $\mathbb{Q}$. Recall that a sequence a_n, $n \in \mathbb{N}$, of rational numbers is called a *Cauchy sequence*, if for every real $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that $|a_m - a_n| \leqslant \epsilon$ for all $m, n \in \mathbb{N}$, $m, n \geqslant N$. Every Cauchy sequence should converge to a limit and it is $\mathbb{R}$ (and not $\mathbb{Q}$) where this happens. Seeing convergence of Cauchy sequences people were not whole-heartedly happy, because the real polynomial $X^2 + 1$ did not have – it continues not to have – roots in $\mathbb{R}$. So the next question that arose was that of *algebraic closure*. $\mathbb{C}$ was invented and turned out to be a nice field which is both algebraically closed and complete. *Voila*!

Throughout the above business we were led by the conventional notion of *distance* between points (i.e., between numbers) – the so-called *Archimedean distance* or the *absolute value*. For every rational prime p there exists a *p-adic distance* which leads to a ring $\hat{\mathbb{Z}}_p$ strictly bigger than and containing $\mathbb{Z}$. This is the ring of *p-adic integers*. The quotient field of $\hat{\mathbb{Z}}_p$ is the field $\mathbb{Q}_p$ of p-adic numbers. $\mathbb{Q}_p$ is complete in the sense of convergence of Cauchy sequences (under the p-adic distance), but is again not algebraically closed. We know anyway that a (unique) algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ exists. We have $[\mathbb{C} : \mathbb{R}] = 2$, i.e., it was necessary and sufficient to add the imaginary quantity i to $\mathbb{R}$ to get an algebraically closed field. Unfortunately in the case of the p-adic distance the closure $\bar{\mathbb{Q}}_p$ is of infinite extension degree over $\mathbb{Q}_p$. In addition $\bar{\mathbb{Q}}_p$ is again not complete. An attempt to make $\bar{\mathbb{Q}}_p$ complete gives an even bigger field Ω_p and the story stops here, Ω_p being both algebraically closed and complete. But Ω_p is already a pretty huge field and very little is known about it.

In this chapter I will introduce the formation of p-adic integers and rationals, prove the completeness of $\mathbb{Q}_p$ and also talk about an important theorem due to Hensel (popularly known as *Hensel's lemma*). In what follows I, without specific mention, will denote by p an arbitrary rational prime.

6.1 Arithmetic of p-adic numbers

There are various ways in which p-adic integers can be defined. A simple (and yet conventional) way is to use infinite sequences.

6.1 Definition A p-adic integer is a defined as an infinite sequence $(a_n) = (a_n)_{n\in\mathbb{N}}$, of elements $a_n \in \mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ with the property that $a_{n+1} \equiv a_n \pmod{p^n}$ for every $n \in \mathbb{N}$. Each a_n, being an element of $\mathbb{Z}_{p^n}$, can be represented as a (rational) integer unique modulo p^n. Thus if b_n, $n \in \mathbb{N}$, is another sequence of integers with $b_n \equiv a_n \pmod{p^n}$ for every n, the p-adic integers (a_n) and (b_n) are treated the same. In particular if $0 \leqslant b_n < p^n$ for every n, then (b_n) is called the canonical representation of (a_n). The set of all p-adic integers is denoted by $\hat{\mathbb{Z}}_p$.[1] A sequence (a_n) of integers with $a_{n+1} \equiv a_n \pmod{p^n}$ for every n is often called a p-coherent sequence.

[1] Well! We are now in a mess of notations. We have $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ for every $n \in \mathbb{N}$. In particular for $p \in \mathbb{P}$ we have $\mathbb{Z}_p$ which is a field that we planned to denote also by $\mathbb{F}_p$. It is superfluous to have two notations for the same thing. Many authors therefore prefer to avoid the hat and call $\hat{\mathbb{Z}}_p$ as $\mathbb{Z}_p$. For them our $\mathbb{Z}_p$ is $\mathbb{F}_p$ and/or $\mathbb{Z}/p\mathbb{Z}$ written explicitly. Let us stick to our old conventions and use hats to remove ambiguities.

See Exercise 6.1.1 for another equivalent way of defining p-adic integers. A homological definition is provided in Exercise 6.1.4, and this definition makes it immediate that $\hat{\mathbb{Z}}_p$ is indeed a ring. However let us proceed in an elementary way by explicitly defining the binary operations on $\hat{\mathbb{Z}}_p$. Before doing that let me mention that the ring $\mathbb{Z}$ is canonically embedded in $\hat{\mathbb{Z}}_p$ under the map $\iota : \mathbb{Z} \to \hat{\mathbb{Z}}_p$, $a \mapsto (a)$. It is easy to see that ι is an injection.

6.2 Definition Let (a_n) and (b_n) be two p-adic integers. Define:

$$\begin{aligned}(a_n) + (b_n) &:= (a_n + b_n).\\ (a_n) \cdot (b_n) &:= (a_n \cdot b_n).\end{aligned}$$

One can easily check that these operations are well-defined, i.e., independent of the choice of the representatives of a_n and b_n. It also follows easily that these operations make $\hat{\mathbb{Z}}_p$ a ring with additive identity $\iota(0) = (0)$ and with multiplicative identity $\iota(1) = (1)$. The additive inverse of (a_n) is $-(a_n) = (-a_n)$. Moreover ι is an injective ring homomorphism $\mathbb{Z} \to \hat{\mathbb{Z}}_p$. In view of this one often identifies the rational integer a with the p-adic integer $\iota(a) = (a)$. We will also do so, provided that we do not expect to face a danger of confusion. Also note that for $l \in \mathbb{Z}$ the l-fold sum $l(a_n)$ is the same as $(l)(a_n) = (la_n)$. Thus in this context the two interpretations of l remain perfectly consistent.

Cool! $\hat{\mathbb{Z}}_p$ is at least a ring. But what kind of ring is it? It turns out that $\hat{\mathbb{Z}}_p$ is an integral domain. In order to see why let us focus our attention on the units of $\hat{\mathbb{Z}}_p$. Let us plan to denote $\hat{\mathbb{Z}}_p^*$ (the multiplicative group of units of $\hat{\mathbb{Z}}_p$) by U_p. The next result characterizes elements of U_p.

6.3 Proposition For $(a_n) \in \hat{\mathbb{Z}}_p$ the following conditions are equivalent:

(a) $(a_n) \in U_p$

(b) $p \not| a_n$ for all $n \in \mathbb{N}$.

(c) $p \not| a_1$.

Proof [(a)⇒(b)] Let $(a_n)(b_n) = (a_n b_n) = 1 = (1)$ for some $(b_n) \in \hat{\mathbb{Z}}_p$. Then for every $n \in \mathbb{N}$ we have $a_n b_n \equiv 1 \pmod{p^n}$, i.e., a_n is invertible modulo p^n and hence modulo p as well, i.e., $p \not| a_n$.

[(b)⇒(c)] Obvious.

[(c)⇒(a)] Let us compute a p-coherent sequence b_n, $n \in \mathbb{N}$, of (rational) integers with $a_n b_n \equiv 1 \pmod{p^n}$. Then (b_n) will be the desired inverse of (a_n) in $\hat{\mathbb{Z}}_p$. Since $p \not| a_1$ and $a_n \equiv a_1 \pmod{p}$, it follows that $p \not| a_n$ as well and therefore the congruence $a_n x \equiv 1 \pmod{p^n}$ has a unique solution modulo p^n, namely $b_n \equiv a_n^{-1} \pmod{p^n}$. We also have $a_{n+1} b_{n+1} \equiv 1 \pmod{p^n}$, i.e., $a_n b_{n+1} \equiv 1 \pmod{p^n}$, i.e., $b_{n+1} \equiv b_n \pmod{p^n}$. ◀

6.4 Proposition Every $0 \neq x = (a_n) \in \hat{\mathbb{Z}}_p$ can be written uniquely as $x = p^r y$ for some $r \in \mathbb{Z}_+$ and for some $y \in U_p$.

Proof If $p \not| a_1$, take $r := 0$ and $y := x$. So assume that $p \mid a_1$. Choose $r \in \mathbb{N}$ such that $[a_n]_{p^n} = [0]_{p^n}$ for $1 \leqslant n \leqslant r$, whereas $[a_{r+1}]_{p^{r+1}} \neq [0]_{p^{r+1}}$. Such an r exists, since $x \neq 0$ by hypothesis. For $n \in \mathbb{N}$ we have $a_{r+n} \equiv a_r \equiv 0 \pmod{p^r}$, i.e., $p^r \mid a_{r+n}$, whereas $a_{r+n} \equiv a_{r+1} \not\equiv 0 \pmod{p^{r+1}}$, i.e., $p^{r+1} \not| a_{r+n}$, i.e., $\mathrm{v}_p(a_{r+n}) = r$. Define $b_n := a_{r+n}/p^r$. Since $a_{r+n+1} \equiv a_{r+n} \pmod{p^{r+n}}$, division by p^r gives $b_{n+1} \equiv b_n \pmod{p^n}$, i.e., $y := (b_n) \in \hat{\mathbb{Z}}_p$. Moreover $p^r b_n = a_{r+n} \equiv a_n \pmod{p^n}$, i.e., $x = p^r y$. Finally since $p \not| b_1$, we have $y \in U_p$. This establishes the existence of a factorization $x = p^r y$. The uniqueness of this factorization is left to the reader as an easy exercise. ◀

6.5 Proposition $\hat{\mathbb{Z}}_p$ is an integral domain.

Proof Let x_1 and x_2 be non-zero elements of $\hat{\mathbb{Z}}_p$. By the previous proposition we can then write $x_1 = p^{r_1}y_1$ and $x_2 = p^{r_2}y_2$ with $r_1, r_2 \in \mathbb{Z}_+$ and $y_1, y_2 \in U_p$. Then $(a_n) := x_1x_2 = p^{r_1+r_2}y_1y_2$. Now $(b_n) := y_1y_2 \in U_p$ and hence no b_n is divisible by p. Therefore $a_{r_1+r_2+1} = p^{r_1+r_2}b_{r_1+r_2+1} \not\equiv 0 \pmod{p^{r_1+r_2+1}}$, i.e., $(a_n) = x_1x_2 \neq 0$. ◀

6.6 Definition The quotient field $\mathbb{Q}_p := \mathrm{Q}(\hat{\mathbb{Z}}_p)$ of $\hat{\mathbb{Z}}_p$ is called the field of p-adic numbers.

6.7 Proposition Every non-zero $x \in \mathbb{Q}_p$ can be expressed uniquely as $x = p^r y$ with $r \in \mathbb{Z}$ and $y \in U_p$.

Proof One can write $x = a/b$ for some $a, b \in \hat{\mathbb{Z}}_p \setminus \{0\}$. Then $a = p^s c$ and $b = p^t d$ for some $s, t \in \mathbb{Z}_+$, $c, d \in U_p$ and so $x = p^{s-t}(c/d)$ with $c/d = cd^{-1} \in U_p$. The proof for the uniqueness is left to the reader. ◀

The canonical inclusion $\iota : \mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}_p$ naturally extends to the canonical inclusion $\iota : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We can identify $\iota(a/b) = \iota(a)/\iota(b) \in \iota(\mathbb{Q}) \subseteq \mathbb{Q}_p$ with the rational a/b and say that $\mathbb{Q}$ is *contained* in $\mathbb{Q}_p$. Being a field of characteristic 0, $\mathbb{Q}_p$ contains an isomorphic copy of $\mathbb{Q}$. The map ι gives this isomorphism explicitly. Note that the ring $\hat{\mathbb{Z}}_p$ is strictly bigger than $\mathbb{Z}$ and the field $\mathbb{Q}_p$ is strictly bigger than the field $\mathbb{Q}$ (Exercise 6.1.6).

Exercises for Section 6.1

1. **(a)** Show that every p-adic integer (a_n) can be *uniquely* described as a sequence $(x_n)_{n\in\mathbb{Z}_+}$ of integers x_n satisfying $0 \leqslant x_n < p$ for every $n \in \mathbb{Z}_+$ and $a_n \equiv x_0 + x_1p + \cdots + x_{n-1}p^{n-1} \pmod{p^n}$ for every $n \in \mathbb{N}$. In this case the p-adic integer (a_n) is written as the *infinite series*

$$(a_n) = x_0 + x_1p + x_2p^2 + \cdots,$$

and one often calls the above series the p-adic expansion of (a_n). Note that the sum in the above series is to be treated as a *formal sum* and not as one of integers. For $a \in \mathbb{N}$ one can find the expansion of a to the base p and this expansion is the same as the p-adic expansion of a (more correctly of $\iota(a) = (a)$).

(b) Given two p-adic integers $a := x_0 + x_1p + x_2p^2 + \cdots$ and $b := y_0 + y_1p + y_2p^2 + \cdots$, find the p-adic integers $c := z_0 + z_1p + z_2p^2 + \cdots$ and $d := w_0 + w_1p + w_2p^2 + \cdots$ such that $c = a + b$ and $d = ab$. (That is, express each z_n and w_n explicitly in terms of x_n's and y_n's.)

2. [Inductive limit] A directed set I is a partially ordered set (under $\leqslant$) with the property that for every $i, j \in I$ one has some $k \in I$ such that $i \leqslant k$ and $j \leqslant k$. Obviously totally ordered sets (like $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$) are directed.

Let I be a directed set, A_i, $i \in I$, a family of rings indexed by I, and $\varphi_{ji} : A_i \to A_j$ a family of ring homomorphisms defined for all $(i, j) \in I^2$ with $i \leqslant j$. Assume further that $\varphi_{ki} = \varphi_{kj} \circ \varphi_{ji}$, whenever $i \leqslant j \leqslant k$, and that $\varphi_{ii} = \mathrm{id}_{A_i}$ for all $i \in I$.

Show that there is a ring A together with ring homomorphisms $\varphi_i : A_i \to A$ such that $\varphi_j \circ \varphi_{ji} = \varphi_i$ for all $i \leqslant j$, and such that A satisfies the following universal property: For every ring B with ring homomorphisms $\psi_i : A_i \to B$ there exists a unique $\psi : A \to B$ such that $\psi \circ \varphi_i = \psi_i$ for all $i \in I$. The ring A is called the colimit or the direct limit or the inductive limit of the rings A_i (under the maps φ_{ji}) and is often denoted by $\varinjlim A_i$.

3. [Projective limit] Let I be a directed set, A_i, $i \in I$, a family of rings indexed by I, and $\varphi_{ij} : A_j \to A_i$ a family of ring homomorphisms defined for all $(i, j) \in I^2$ with $i \leqslant j$. Assume further that $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$, whenever $i \leqslant j \leqslant k$, and that $\varphi_{ii} = \mathrm{id}_{A_i}$ for all $i \in I$.

Show that there is a ring A together with ring homomorphisms $\varphi_i : A \to A_i$ such that $\varphi_{ij} \circ \varphi_j = \varphi_i$ for all $i \leqslant j$, and such that A satisfies the following universal property: For every ring B with ring homomorphisms $\psi_i : B \to A_i$ there exists a unique $\psi : B \to A$ such that $\varphi_i \circ \psi = \psi_i$ for all $i \in I$. The ring A is called the inverse limit or the projective limit or simply the limit of the rings A_i (under the maps φ_{ij}) and is often denoted by $\varprojlim A_i$.

4. Show that the ring $\hat{\mathbb{Z}}_p$ of p-adic integers is isomorphic to the projective limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ of the rings $\mathbb{Z}/p^n\mathbb{Z}, n \in \mathbb{N}$, under the canonical surjections $\varphi_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, $[a]_{p^n} \mapsto [a]_{p^m}$, for all $m, n \in \mathbb{N}$, $m \leqslant n$.

5. Let p be an odd prime and $a \in \mathbb{Z}$ with $\left(\frac{a}{p}\right) = 1$. From elementary number theory we know that the congruence $x^2 \equiv a \pmod{p^n}$ has two solutions for every $n \in \mathbb{N}$. Let x_1 be a solution of $x^2 \equiv a \pmod{p}$. We know that a solution x_n of $x^2 \equiv a \pmod{p^n}$ *lifts* uniquely to a solution x_{n+1} of $x^2 \equiv a \pmod{p^{n+1}}$. Thus we can inductively compute a sequence $x_1, x_2, x_3, \ldots$ of integers. Show that (x_n) is a p-adic integer and that $(x_n)^2 = (a)$.

6. **(a)** Show that the ring $\hat{\mathbb{Z}}_p$ *contains* rationals of the form a/b, $a, b \in \mathbb{Z}, p\not| b$. This implies that $\mathbb{Z} \subsetneqq \hat{\mathbb{Z}}_p$.

(b) Take $a := 17$ for $p = 2$, $a := 7$ for $p = 3$ and $a := p + 1$ for $p > 3$. Show that there exists $x \in \mathbb{Q}_p$ with $x^2 = a$ in $\mathbb{Q}_p$. Show that such an x does not belong to $\mathbb{Q}$. Thus $\mathbb{Q} \subsetneqq \mathbb{Q}_p$.

(c) Show that $1/p \in \mathbb{Q}_p \setminus \hat{\mathbb{Z}}_p$. Thus $\hat{\mathbb{Z}}_p \subsetneqq \mathbb{Q}_p$.

6.2 p-adic valuation

Proposition 6.7 leads to the notion of the p-adic distance between pairs of points in $\mathbb{Q}_p$. Let us start with some formal definitions.

6.8 Definition A metric on a set S is a map $d : S \times S \to \mathbb{R}$ such that for every $x, y, z \in S$ we have:

(1) [Non-negative] $d(x, y) \geqslant 0$.

(2) [Non-degeneracy] $d(x, y) = 0$, if and only if $x = y$.

(3) [Symmetry] $d(x, y) = d(y, x)$.

(4) [Triangle inequality] $d(x, z) \leqslant d(x, y) + d(y, z)$.

A set S together with a metric d on S is called a metric space (with metric d).

6.9 Definition A norm on a field K is a map $|| \quad || : K \to \mathbb{R}$ such that for all $x, y \in K$ we have:

(1) [Non-negative] $||x|| \geqslant 0$.

(2) [Non-degeneracy] $||x|| = 0$, if and only if $x = 0$.

(3) [Multiplicativity] $||xy|| = ||x|| \, ||y||$.

(4) [Triangle inequality] $||x + y|| \leqslant ||x|| + ||y||$.

It is an easy check that for a norm $|| \quad ||$ on K the function $d : K \times K \to \mathbb{R}$, $d(x, y) := ||x - y||$, defines a metric on K.

A norm $|| \quad ||$ on a field K is called non-Archimedean (or a finite valuation), if $||x + y|| \leqslant \max(||x||, ||y||)$ for all $x, y \in K$ (a condition stronger than the triangle inequality). A norm which is not non-Archimedean is called Archimedean (or an infinite valuation).

6.10 Example (1) One can easily verify that setting $||x|| := \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0, \end{cases}$ defines a norm on any field K. This norm is called the trivial norm on K.

(2) The absolute value $| \quad |$ is an *Archimedean norm* on $\mathbb{Q}$ (or $\mathbb{R}$), as one can easily verify. It is often customary to denote this norm as $| \quad |_\infty$. This norm induces the usual metric topology on $\mathbb{Q}$ (or $\mathbb{R}$) which is at the heart of real analysis. In p-adic analysis one investigates $\mathbb{Q}$ under the p-adic norms that I am going to define now.

6.11 Definition The *p-adic norm* $|\ |_p : \mathbb{Q}_p \to \mathbb{R}$ on $\mathbb{Q}_p$ is defined as:

$$|x|_p := \begin{cases} 0 & \text{if } x = 0, \\ p^{-r} & \text{if } x = p^r y \text{ with } r \in \mathbb{Z} \text{ and } y \in U_p. \end{cases}$$

The restriction of $|\ |_p$ to $\mathbb{Q}$ is often denoted by the same symbol.

6.12 Theorem The p-adic norm $|\ |_p$ is a non-Archimedean norm on $\mathbb{Q}_p$ (as well as on $\mathbb{Q}$).

Proof Non-negative-ness, non-degeneracy and multiplicativity of $|\ |_p$ are immediate. For proving the triangle inequality it is sufficient to prove the non-Archimedean condition. Take $x, y \in \mathbb{Q}_p$. If $x = 0$ or $y = 0$ or $x + y = 0$, we clearly have $|x + y|_p \leqslant \max(|x|_p, |y|_p)$. So assume that each of x, y and $x + y$ is non-zero. Write $x = p^r u$ and $y = p^s v$ with $r, s \in \mathbb{Z}$ and $u, v \in U_p$. Without loss of generality we can assume that $r \geqslant s$. Then $x + y = p^s z$, where $z := p^{r-s}u + v \in \hat{\mathbb{Z}}_p$. Since $x + y \neq 0$, we have $z \neq 0$, so that we can write $z = p^t w$ for some $t \in \mathbb{Z}_+$ and $w \in U_p$. But then $|x + y|_p = p^{-(s+t)} \leqslant p^{-s} = \max(p^{-r}, p^{-s}) = \max(|x|_p, |y|_p)$. ◀

6.13 Definition Two metrics d_1 and d_2 on a metric space S are said to be *equivalent*, if a sequence (x_n) from S is Cauchy with respect to d_1, if and only if it is Cauchy with respect to d_2. Two norms on a field are said to be equivalent, if they give rise to equivalent metrics on K.

Note that for every $p \in \mathbb{P}$ the field $\mathbb{Q}$ is canonically embedded in $\mathbb{Q}_p$ and thus we have a notion of a p-adic *distance* on $\mathbb{Q}$. We also have the usual Archimedean distance $|\ |_\infty$ on $\mathbb{Q}$. I will now state an interesting result without a proof, which asserts that any distance on $\mathbb{Q}$ must be essentially the same as either the usual Archimedean distance or one of the p-adic distances.

6.14 Theorem [Ostrowski's theorem] Every non-trivial norm on $\mathbb{Q}$ is equivalent to $|\ |_p$ for some $p \in \mathbb{P} \cup \{\infty\}$. ◀

The notions of sequences and series and their convergences can be readily extended to $\mathbb{Q}_p$ under the norm $|\ |_p$. Since the p-adic distance assumes only the discrete values p^r, $r \in \mathbb{Z}$, it is often customary to restrict ourselves only to these values while talking about the convergence criteria of sequences and series, i.e., instead of an infinitesimally small real $\epsilon > 0$ one can talk about an arbitrarily large $M \in \mathbb{N}$ with $p^{-M} \leqslant \epsilon$.

6.15 Definition Let $x_1, x_2, \ldots$ be a sequence of elements of $\mathbb{Q}_p$. We say that this sequence *converges* to a *limit* $x \in \mathbb{Q}_p$, if given any $M \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that $|x_n - x|_p \leqslant p^{-M}$ for all $n \geqslant N$. In this case we write $x = \lim x_n$ and also $x_n \to x$.

Consider the partial sums $s_n := x_1 + \cdots + x_n \in \mathbb{Q}_p$ for each $n \in \mathbb{N}$. If there exists $s \in \mathbb{Q}_p$ with $s_n \to s$, we say that the *sum* $\sum_{n \in \mathbb{N}} x_n$ *converges* to s and write $s = \sum_{n \in \mathbb{N}} x_n$.

A sequence $x_1, x_2, \ldots$ of elements of $\mathbb{Q}_p$ is said to be a *Cauchy sequence*, if for every $M \in \mathbb{N}$ there exists an $N \in \mathbb{N}$ such that $|x_m - x_n|_p \leqslant p^{-M}$ for all $m, n \geqslant N$.

A field K with a norm $||\ ||$ is called *complete* (under the given norm), if every sequence of elements of K, which is Cauchy under $||\ ||$, converges to an element in K. For example $\mathbb{R}$ is complete under $|\ |_\infty$. I will shortly demonstrate that $\mathbb{Q}_p$ is complete under $|\ |_p$.

Consider a field K not (necessarily) complete under a norm $||\ ||$. Let C denote the set of all Cauchy sequences $(a_n) = (a_n)_{n \in \mathbb{N}}$ from K. Define addition and multiplication in C as $(a_n) + (b_n) := (a_n + b_n)$

and $(a_n)(b_n) := (a_n b_n)$. Under these operations C becomes a commutative ring with identity having a maximal ideal $\mathfrak{m} := \{(a_n) \mid a_n \to 0\}$. The field $L := C/\mathfrak{m}$ is called the completion of K with respect to the norm $|| \;\; ||$. K is canonically embedded in L via the map $x \mapsto (x) + \mathfrak{m}$. The norm $|| \;\; ||$ on K extends to elements $(a_n) + \mathfrak{m}$ of L as $\lim_{n\to\infty} ||a_n||$. L is a complete field under this extended norm. In fact it is the smallest field containing K and complete under $|| \;\; ||$.

$\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the Archimedean norm $| \;\; |_\infty$. On the other hand, $\mathbb{Q}_p$ turns out to be the completion of $\mathbb{Q}$ with respect to the p-adic norm $| \;\; |_p$. Before proving this let us first prove that $\mathbb{Q}_p$ itself is a complete field under the p-adic norm. Let us start with a lemma.

6.16 Lemma Let (a_n) be a sequence of p-adic numbers. Then (a_n) is Cauchy, if and only if the sequence $(a_{n+1} - a_n)$ converges to 0.

Proof [if] Take any $M \in \mathbb{N}$. Since $a_{n+1} - a_n \to 0$ by hypothesis, there exists $N \in \mathbb{N}$ such that $|a_{n+1} - a_n|_p \leqslant p^{-M}$ for all $n \geqslant N$. But then for all $m, n \geqslant N$ with $m = n + k$, $k \in \mathbb{N}$, we have $|a_m - a_n|_p = \left|\sum_{i=0}^{k-1}(a_{n+i+1} - a_{n+i})\right|_p \leqslant \max_{0\leqslant i\leqslant k-1} |a_{n+i+1} - a_{n+i}|_p \leqslant p^{-M}$. Thus (a_n) is a Cauchy sequence.

[only if] Take any $M \in \mathbb{N}$. Since (a_n) is a Cauchy sequence by hypothesis, there exists $N \in \mathbb{N}$ such that $|a_m - a_n|_p \leqslant p^{-M}$ for all $m, n \geqslant N$. In particular $|a_{n+1} - a_n|_p \leqslant p^{-M}$ for all $n \geqslant N$, i.e., $a_{n+1} - a_n \to 0$. ◀

6.17 Theorem The field $\mathbb{Q}_p$ is complete with respect to $| \;\; |_p$.

Proof Let (a_n) be a Cauchy sequence in $\mathbb{Q}_p$. By the previous lemma $a_{n+1} - a_n \to 0$. Therefore there exists $N \in \mathbb{N}$ such that $|a_{n+1} - a_n|_p \leqslant 1$ for all $n \geqslant N$. For $n = N + k$, $k \in \mathbb{N}$, we have

$$\begin{aligned} |a_n|_p &= |a_{N+k}|_p \\ &= |(a_{N+k} - a_{N+k-1}) + \cdots + (a_{N+1} - a_N) + a_N|_p \\ &\leqslant \max(|a_{N+k} - a_{N+k-1}|_p, \ldots, |a_{N+1} - a_N|_p, |a_N|_p) \\ &\leqslant \max(1, |a_N|_p). \end{aligned}$$

It follows that $|a_n|_p \leqslant p^{-m}$ for all $n \in \mathbb{N}$, where $m \in \mathbb{Z}$ satisfies $p^{-m} = \max(1, |a_1|_p, \ldots, |a_N|_p)$. If $m \geqslant 0$, then each $a_n \in \hat{\mathbb{Z}}_p$ (Exercise 6.2.1). Otherwise consider the sequence $(p^{-m}a_n)$ which is clearly Cauchy and in which each $p^{-m}a_n \in \hat{\mathbb{Z}}_p$, since $|p^{-m}a_n|_p \leqslant p^m p^{-m} = 1$. Thus without loss of generality we can assume that the given sequence (a_n) itself is one of p-adic *integers*.

Let $a_n = a_{n,0} + a_{n,1}p + a_{n,2}p^2 + \cdots$ be the p-adic expansion of a_n (Exercise 6.2.2). Since (a_n) is Cauchy, for every $M \in \mathbb{Z}_+$ there exists $N_M \in \mathbb{N}$ such that $|a_m - a_n|_p \leqslant p^{-(M+1)}$ for all $m, n \geqslant N_M$, i.e., $a_{n,i} = a_{m,i}$ for $0 \leqslant i \leqslant M$, $m, n \geqslant N_M$. Define $x_M := a_{n,M}$ for any $n \geqslant N_M$ and $x := x_0 + x_1 p + x_2 p^2 + \cdots \in \hat{\mathbb{Z}}_p$. It then follows that $a_n \to x$. ◀

6.18 Theorem $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the norm $| \;\; |_p$.

Proof As above let C denote the ring of Cauchy sequences from $\mathbb{Q}$ (under the p-adic norm), $\mathfrak{m}$ the maximal ideal of C consisting of sequences that converge to 0, and let $L := C/\mathfrak{m}$. I will now show that $L \cong \mathbb{Q}_p$.

If $a \in \mathbb{Q}_p$ has the p-adic expansion $a = a_{-r}p^{-r} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots$ (Exercise 6.2.2), then $\alpha_n := a_{-r}p^{-r} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots + a_n p^n$, $n \in \mathbb{N}$, define a sequence of elements of $\mathbb{Q}$. We have $|\alpha_n - a|_p \leqslant p^{-(n+1)}$, i.e., $\alpha_n \to a$. Moreover the sequence (α_n) of rational numbers is Cauchy with respect to $|\ \ |_p$, since for every $M \in \mathbb{N}$ we have $|\alpha_m - \alpha_n|_p \leqslant p^{-(M+1)}$ for all $m, n \geqslant M$. Thus $\varphi : \mathbb{Q}_p \to L$, $a \mapsto (\alpha_n) + \mathfrak{m}$, is a well-defined field homomorphism. Being a field homomorphism φ is injective.

What remains is to show that the map φ is surjective. Take any $(\beta_n) + \mathfrak{m} \in L$. Since (β_n) is a Cauchy sequence, by Theorem 6.17 it converges to a point $a \in \mathbb{Q}_p$. We construct the sequence (α_n) corresponding to a as described in the last paragraph. Then $\alpha_n \to a$ as well and hence using the triangle inequality (or the non-Archimedean condition) we have $\alpha_n - \beta_n = (\alpha_n - a) - (\beta_n - a) \to 0$, i.e., $(\alpha_n) - (\beta_n) = (\alpha_n - \beta_n) \in \mathfrak{m}$, i.e., $\varphi(a) = (\alpha_n) + \mathfrak{m} = (\beta_n) + \mathfrak{m}$. ◀

6.19 Corollary The p-adic series $\sum_{n\in\mathbb{N}} a_n$ (with $a_n \in \mathbb{Q}_p$) converges, if and only if $|a_n|_p \to 0$.

Proof The 'only if' part is obvious. For the 'if' part take a sequence (a_n) of p-adic numbers with $|a_n|_p \to 0$. Define $s_n := \sum_{i=1}^{n} a_n$. Since $a_{n+1} = s_{n+1} - s_n \to 0$ by hypothesis, Lemma 6.16 guarantees that (s_n) is a Cauchy sequence, i.e., (s_n) converges in $\mathbb{Q}_p$. ◀

This is quite unlike the Archimedean norm $|\ \ |_\infty$. For example, with respect to this norm $\frac{1}{n} \to 0$, whereas the series $\sum_{n\in\mathbb{N}} \frac{1}{n}$ diverges.

Exercises for Section 6.2

1. Prove the following assertions:

(a) $\hat{\mathbb{Z}}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leqslant 1\}$.

(b) $U_p = \{x \in \mathbb{Q}_p \mid |x|_p = 1\}$.

(c) Every non-zero ideal of $\hat{\mathbb{Z}}_p$ is of the form $\mathfrak{a}_r := \{x \in \hat{\mathbb{Z}}_p \mid |x|_p \leqslant p^{-r}\}$ for some $r \in \mathbb{Z}_+$.

(d) The ideals $\mathfrak{a}_r$ of Part (c) satisfy the infinite strictly descending chain $\hat{\mathbb{Z}}_p = \mathfrak{a}_0 \supsetneqq \mathfrak{a}_1 \supsetneqq \mathfrak{a}_2 \supsetneqq \cdots$.

(e) $\hat{\mathbb{Z}}_p$ is a local domain with the maximal ideal $\mathfrak{m}_p := \mathfrak{a}_1 = \{x \in \hat{\mathbb{Z}}_p \mid |x|_p < 1\}$.

(f) The ideal $\mathfrak{a}_r$ of Part (c) is the principal ideal of $\hat{\mathbb{Z}}_p$ generated by p^r and $\hat{\mathbb{Z}}_p/\mathfrak{a}_r \cong \mathbb{Z}/p^r\mathbb{Z}$. In particular $\hat{\mathbb{Z}}_p$ is a local PID (i.e., a discrete valuation domain) with the residue field $\hat{\mathbb{Z}}_p/\mathfrak{m}_p \cong \mathbb{F}_p$.

2. In view of Exercise 6.1.1 every $x \in \hat{\mathbb{Z}}_p$ admits a unique expansion of the form $x = x_0 + x_1 p + x_2 p^2 + \cdots$, where each $x_i \in \{0, 1, \ldots, p-1\}$. This notion of p-adic expansion can be extended to the elements of $\mathbb{Q}_p$.

(a) Show that for every $x \in \mathbb{Q}_p \setminus \hat{\mathbb{Z}}_p$ there exist unique $r \in \mathbb{N}$ and unique integers $x_{-r}, x_{-r+1}, \ldots, x_{-1}, x_0, x_1, \ldots$, each in $\{0, 1, \ldots, p-1\}$, such that x can be represented as:

$$x = x_{-r}p^{-r} + x_{-r+1}p^{-r+1} + \cdots + x_{-1}p^{-1} + x_0 + x_1 p + x_2 p^2 + \cdots .$$

(b) Describe how to compute the p-adic expansions of $x + y$ and xy given those for $x, y \in \mathbb{Q}_p$. Also of x/y provided that $y \neq 0$.

(c) What is $|x|_p$ for $x := x_0 + x_1 p + x_2 p^2 + \cdots \in \hat{\mathbb{Z}}_p$?

(d) What is $|x|_p$ for $x := x_{-r}p^{-r} + x_{-r+1}p^{-r+1} + \cdots + x_{-1}p^{-1} + x_0 + x_1 p + x_2 p^2 + \cdots \in \mathbb{Q}_p$ with $x_{-r} \neq 0$.

3. Compute the p-adic expansion of $1/3$ in $\mathbb{Q}_5$ and of $-2/5$ in $\mathbb{Q}_3$.

4. Show that $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}_p$ under the p-adic norm $|\ \ |_p$, i.e., show that given any $x \in \hat{\mathbb{Z}}_p$ and real $\epsilon > 0$ there exists $a \in \mathbb{Z}$ such that $|x - a|_p < \epsilon$. Show also that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

5. Prove the following assertions that establish that $\hat{\mathbb{Z}}_p$ is the *closure* of $\mathbb{Z}$ in $\mathbb{Q}_p$ with respect to $|\ \ |_p$.

(a) Every sequence (a_n) of rational integers, Cauchy with respect to $|\ \ |_p$, converges in $\hat{\mathbb{Z}}_p$.

(b) If a sequence (a_n) of rational numbers, Cauchy with respect to $|\ \ |_p$, converges to a point $x \in \hat{\mathbb{Z}}_p$, then there exists a sequence (b_n) of rational integers, Cauchy with respect to $|\ \ |_p$, that converges to x.

6. Show that:

(a) The series $\sum_{n\in\mathbb{N}} n!$ converges in $\mathbb{Q}_p$.

(b) The series $\sum_{n\in\mathbb{N}} n\cdot n!$ converges in $\mathbb{Q}_p$.

(c) $\sum_{n\in\mathbb{N}} n\cdot n! = -1$ in $\mathbb{Q}_p$. (**Hint:** First show that $\sum_{i=1}^{n} i\cdot i! = (n+1)!-1$.)

(d) The series $\sum_{n\in\mathbb{N}} \frac{1}{n}$ does not converge in $\mathbb{Q}_p$.

(e) If $a\in\mathbb{Q}_p$ and $|a|_p<1$, then $\frac{1}{1-a} = 1+a+a^2+\cdots$.

7. Prove that $\displaystyle\prod_{p\in\mathbb{P}\cup\{\infty\}} |a|_p = 1$ for any non-zero $a\in\mathbb{Q}$. (**Hint:** Use unique factorization of rationals.)

8. Demonstrate that for any $a\in\hat{\mathbb{Z}}_p$ the sequence (a^{p^n}) converges in $\mathbb{Q}_p$. (**Hint:** Show by induction on n that p^{n+1} divides $a^{p^{n+1}} - a^{p^n}$ in $\hat{\mathbb{Z}}_p$ for all $n\in\mathbb{N}$.)

9. Show that $\hat{\mathbb{Z}}_p \cong \mathbb{Z}[[X]]/\langle X-p\rangle$, where $\mathbb{Z}[[X]]$ denotes the ring of all formal power series in one variable X and with coefficients from $\mathbb{Z}$. (**Hint:** Consider the map $a_0+a_1X+a_2X^2+\cdots \mapsto \bar{a}_0+\bar{a}_1p+\bar{a}_2p^2+\cdots$, where $\bar{a}_n\equiv a_n \pmod p$ and $0\leqslant \bar{a}_n < p$.)

*** 10.** Let $p,q\in\mathbb{P}$, $p\neq q$. Show that the fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic.

6.3 Hensel's lemma

Let us conclude our short study of p-adic methods by proving an important theorem due to Hensel. This theorem talks about the solvability of polynomial equations $f(X)=0$ for $f(X)\in\hat{\mathbb{Z}}_p[X]$. Before proceeding further let me introduce a notation. Recall that every $x\in\hat{\mathbb{Z}}_p$ has a unique p-adic expansion of the form $a=a_0+a_1p+a_2p^2+\cdots$ with $0\leqslant a_n<p$ (Exercises 6.1.1 and 6.2.2). If $a_0=a_1=\cdots=a_{n-1}=0$, then $a=a_np^n+a_{n+1}p^{n+1}+a_{n+2}p^{n+2}+\cdots = p^nb$, where $b:=a_n+a_{n+1}p+a_{n+2}p^2+\cdots\in\hat{\mathbb{Z}}_p$. Thus $p^n \mid a$ in $\hat{\mathbb{Z}}_p$. We denote this by saying that $a\equiv 0 \pmod{p^n}$. Notice that $a\equiv 0\pmod{p^n}$, if and only if $|a|_p\leqslant p^{-n}$. We write $a\equiv b\pmod{p^n}$ for $a,b\in\hat{\mathbb{Z}}_p$, if $a-b\equiv 0\pmod{p^n}$. Since p^n can be viewed as the element $\iota(p^n)$ of $\hat{\mathbb{Z}}_p$, these congruence notations conform with that for a general PID. ($\hat{\mathbb{Z}}_p$ is a PID by Exercise 6.2.1.)

Since by our assumption any ring A comes with identity (that we denote by $1=1_A$), it makes sense to talk for every $n\in\mathbb{Z}$ about an element $n=n_A$ in A, which is the n-fold sum of 1. More precisely:

$$n := \begin{cases} 0 & \text{if } n=0,\\ 1+1+\cdots+1 \ (n \text{ times}) & \text{if } n>0,\\ -(-n) & \text{if } n<0.\end{cases}$$

Thus given any $f(X)=a_0+a_1X+a_2X^2+\cdots+a_dX^d\in A[X]$ one can define the formal derivative of f as $f'(X):=a_1+2a_2X+\cdots+da_dX^{d-1}\in A[X]$. Properties of formal derivatives of polynomials are covered in Exercise 1.4.3.

6.20 Theorem [Hensel's lemma] Let $f(X)\in\hat{\mathbb{Z}}_p[X]$. Suppose that there exist $M\in\mathbb{Z}_+$ and $\alpha_0\in\hat{\mathbb{Z}}_p$ satisfying:

(1) $|f(\alpha_0)|_p\leqslant p^{-(2M+1)}$ (i.e., α_0 is a solution of $f(x)\equiv 0 \pmod{p^{2M+1}}$), and

(2) $|f'(\alpha_0)|_p = p^{-M}$ (i.e., $f'(\alpha_0)\not\equiv 0\pmod{p^{M+1}}$).

Then there exists a unique $\alpha\in\hat{\mathbb{Z}}_p$ such that $f(\alpha)=0$ and $|\alpha-\alpha_0|_p\leqslant p^{-(M+1)}$ (i.e., $\alpha\equiv\alpha_0\pmod{p^{M+1}}$).

Proof Let us inductively construct a sequence $\alpha_0,\alpha_1,\alpha_2,\ldots$ of p-adic integers with the properties that $|f(\alpha_n)|_p\leqslant p^{-(2M+n+1)}$ and $|f'(\alpha_n)|_p=p^{-M}$ for every $n\in\mathbb{Z}_+$. The given α_0 provides the starting point (induction basis). For the inductive step assume that $n \geqslant 1$ and that $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ have been constructed with the desired properties. I will now explain how to construct α_n from the knowledge of α_{n-1}. Put

$$\alpha_n := \alpha_{n-1} + k_n p^{M+n} \tag{6.1}$$

for some $k_n \in \hat{\mathbb{Z}}_p$. We want to find a suitable k_n for which $|f(\alpha_n)|_p \leqslant p^{-(2M+n+1)}$. By Taylor expansion we get $f(\alpha_n) = f(\alpha_{n-1}) + k_n p^{M+n} f'(\alpha_{n-1}) + c_n p^{2(M+n)}$ for some $c_n \in \hat{\mathbb{Z}}_p$. Since by induction hypothesis $p^{2M+n} \mid f(\alpha_{n-1})$ and $p^M \mid f'(\alpha_{n-1})$, we can write $f(\alpha_n) = p^{2M+n}\left(\frac{f(\alpha_{n-1})}{p^{2M+n}} + k_n \frac{f'(\alpha_{n-1})}{p^M} + c_n p^n\right)$. Since $p^{M+1} \nmid f'(\alpha_{n-1})$, the element $\frac{f'(\alpha_{n-1})}{p^M} \in U_p$ and therefore there is a unique solution for k_n of the congruence

$$\frac{f(\alpha_{n-1})}{p^{2M+n}} + k_n \frac{f'(\alpha_{n-1})}{p^M} \equiv 0 \pmod{p}. \tag{6.2}$$

As desired this choice of k_n gives $f(\alpha_n) = p^{2M+n}(b_n p + c_n p^n) \equiv 0 \pmod{p^{2M+n+1}}$ for some $b_n \in \hat{\mathbb{Z}}_p$. Moreover the Taylor expansion of f' gives $f'(\alpha_n) = f'(\alpha_{n-1}) + d_n p^{M+n}$ (for some $d_n \in \hat{\mathbb{Z}}_p$) which implies that $f'(\alpha_n) \equiv f'(\alpha_{n-1}) \pmod{p^M}$, i.e., $|f'(\alpha_n)|_p = p^{-M}$.

Since $|\alpha_n - \alpha_{n-1}|_p \leqslant p^{-(M+n)}$, it follows that $\alpha_n - \alpha_{n-1} \to 0$, i.e., (α_n) is a Cauchy sequence (under $|\ \ |_p$). By the completeness of $\mathbb{Q}_p$ we then have an $\alpha \in \mathbb{Q}_p$ such that $\alpha_n \to \alpha$. Similarly $f(\alpha_n) - f(\alpha_{n-1}) \to 0$, i.e., the sequence $(f(\alpha_n))$ is Cauchy and hence converges to $f(\alpha)$. Also $|f(\alpha_n)|_p \leqslant p^{-(2M+n+1)}$, i.e., $f(\alpha_n) \to 0$, i.e., $f(\alpha) = 0$. Finally each $\alpha_n \equiv \alpha_0 \pmod{p^{M+1}}$, so that $\alpha \equiv \alpha_0 \pmod{p^{M+1}}$. This establishes the existence of a desired $\alpha \in \mathbb{Q}_p$.

For proving the uniqueness of α let $\beta \in \mathbb{Q}_p$ satisfy $f(\beta) = 0$ and $|\beta - \alpha_0|_p \leqslant p^{-(M+1)}$. By Taylor expansion $f(\beta) = f(\alpha) + (\beta - \alpha)f'(\alpha) + (\beta - \alpha)^2 c$ for some $c \in \hat{\mathbb{Z}}_p$, i.e., $(\beta - \alpha)(f'(\alpha) + (\beta - \alpha)c) = 0$. Now $\beta - \alpha = (\beta - \alpha_0) - (\alpha - \alpha_0)$ and so $|\beta - \alpha|_p \leqslant \max(|\beta - \alpha_0|_p, |\alpha - \alpha_0|_p) \leqslant p^{-(M+1)}$, whereas $f'(\alpha_n) \to f'(\alpha)$ so that $|f'(\alpha)|_p = p^{-M}$. Therefore $f'(\alpha) + (\beta - \alpha)c \not\equiv 0 \pmod{p^{M+1}}$ and in particular $f'(\alpha) + (\beta - \alpha)c \neq 0$. Thus we must have $\beta - \alpha = 0$. ◀

Note that α_n in the last proof satisfies the congruence $f(\alpha_n) \equiv 0 \pmod{p^{2M+n+1}}$ for each $n \in \mathbb{Z}_+$. We are given the solution α_0 corresponding to $n = 0$. From this we inductively construct the solutions $\alpha_1, \alpha_2, \ldots$ corresponding to $n = 1, 2, \ldots$ respectively. The process for computing α_n from α_{n-1} as described in the proof of Hensel's lemma is often referred to as Hensel lifting. The given conditions ensure that this lifting is possible (and uniquely doable) for every $n \in \mathbb{N}$, and in the limit $n \to \infty$ we get a root $\alpha \in \hat{\mathbb{Z}}_p$ of f. The root α admits a p-adic expansion of the form $\alpha = \alpha_0 + k_1 p^{M+1} + k_2 p^{M+2} + k_3 p^{M+3} + \cdots$, where k_n is obtained by solving (6.2). Since each k_n is required modulo p, we can take $k_n \in \{0, 1, \ldots, p-1\}$.

The special case of Hensel's lemma corresponding to $M = 0$ is often singled out as follows:

6.21 Corollary Let $f(X) \in \hat{\mathbb{Z}}_p[X]$. Suppose that there exists an $\alpha_0 \in \hat{\mathbb{Z}}_p$ satisfying:

(1) $|f(\alpha_0)|_p < 1$ (i.e., α_0 is a solution of $f(x) \equiv 0 \pmod{p}$), and

(2) $|f'(\alpha_0)|_p = 1$ (i.e., $f'(\alpha_0) \not\equiv 0 \pmod{p}$, i.e., α_0 is a *simple root* of f modulo p).

Then there exists a unique $\alpha \in \hat{\mathbb{Z}}_p$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0|_p < 1$ (i.e., $\alpha \equiv \alpha_0 \pmod{p}$). ◀

For this special case we compute solutions α_n of $f(x) \equiv 0 \pmod{p^{n+1}}$ inductively for $n = 1, 2, 3, \ldots$ given a suitable solution α_0 of this congruence for $n = 0$. The lifting formula is now:

$$\alpha_n = \alpha_{n-1} + k_n p^n, \quad \text{where} \quad k_n \equiv -f'(\alpha_{n-1})^{-1}\left(\frac{f(\alpha_{n-1})}{p^n}\right) \pmod{p}. \tag{6.3}$$

6.22 Example $\mathbb{Z}$ is canonically embedded in $\hat{\mathbb{Z}}_p$ and so is $\mathbb{Z}[X]$ in $\hat{\mathbb{Z}}_p[X]$. Thus we often carry out the lifting process for a polynomial $f(X) \in \mathbb{Z}[X]$ and for some solution of $f(X) \equiv 0 \pmod{p}$ in $\mathbb{Z}$. Then one solves (6.3) in $\mathbb{Z}$ and obtains each $\alpha_n \in \mathbb{Z}$. The limit α belongs to $\hat{\mathbb{Z}}_p$ and is a solution of $f(X) = 0$ in $\hat{\mathbb{Z}}_p$.

For example let p be an *odd* prime and $\left(\frac{a}{p}\right) = 1$. Then there is a solution $\alpha_0 \in \mathbb{Z}$ of $x^2 \equiv a \pmod{p}$. Here $f(X) = X^2 - a$, so that $f'(X) = 2X$, i.e., $f'(\alpha_0) = 2\alpha_0 \not\equiv 0 \pmod{p}$. Thus the conditions of Corollary 6.21 are satisfied and we get a unique square root of α in $\hat{\mathbb{Z}}_p$ with $\alpha \equiv \alpha_0 \pmod{p}$. This α has a p-adic expansion of the form $\alpha = \alpha_0 + k_1 p + k_2 p^2 + k_3 p^3 + \cdots$.

As a specific numerical example take $p = 7$, $a = 2$ and $\alpha_0 = 3$. Using the formula (6.3) we compute $k_1 = 1$, $\alpha_1 = 10$, $k_2 = 2$, $\alpha_2 = 108$, $k_3 = 6$, $\alpha_3 = 2166$, and so on. Thus a square root of 2 in $\mathbb{Q}_7$ is $3 + 1 \times 7 + 2 \times 7^2 + 6 \times 7^3 + \cdots$. The other square root of α in $\mathbb{Q}_7$ can be obtained by starting with $\alpha_0 = 4$.

Exercises for Section 6.3

1. Let a be an integer congruent to 1 modulo 8. Show that there exists an $\alpha \in \hat{\mathbb{Z}}_2$ such that $\alpha^2 = a$ and $|\alpha - 1|_2 \leqslant \frac{1}{4}$.

2. Compute $\alpha \in \hat{\mathbb{Z}}_3$ with $\alpha^2 + \alpha + 223 = 0$ and $\alpha \equiv 4 \pmod{243}$.

3. Let p be an odd prime and $a \in \{0, 1, \ldots, p-1\}$. Show that the polynomial $X^2 - a$ has exactly $1 + \left(\frac{a}{p}\right)$ roots in $\hat{\mathbb{Z}}_p$.

4. Show that the polynomial $X^2 - p$ is irreducible in $\hat{\mathbb{Z}}_p[X]$.

5. Let $a \in \mathbb{Z}, 0 \leqslant a < p$. Show that there exists a unique $\alpha \in \hat{\mathbb{Z}}_p$ such that $\alpha^p = \alpha$ and $\alpha \equiv a \pmod{p}$.

6. Prove the following polynomial form of Hensel's lemma:

Let $f(X) \in \hat{\mathbb{Z}}_p[X]$. Suppose that there exists $g_0(X), h_0(X) \in \hat{\mathbb{Z}}_p[X]$ with the properties:
(1) g_0 is monic,
(2) $\gcd(g_0(X), h_0(X)) = 1$ in $\hat{\mathbb{Z}}_p[X]$, and
(3) $f(X) \equiv g_0(X) h_0(X) \pmod{p}$.

Then there exist $g(X), h(X) \in \hat{\mathbb{Z}}_p[X]$ such that g is monic, $f(X) = g(X)h(X)$, $g(X) \equiv g_0(X) \pmod{p}$ and $h(X) \equiv h_0(X) \pmod{p}$.

(**Remark:** This result guarantees that a suitable monic divisor $g_0(X)$ of $f(X)$ modulo p lifts to a monic divisor $g_n(X)$ of $f(X)$ modulo p^{n+1} for every $n \in \mathbb{N}$. In the limit $n \to \infty$ we get a monic divisor $g(X)$ of $f(X)$ in $\hat{\mathbb{Z}}_p[X]$.)

7. Show that the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is of infinite extension degree over $\mathbb{Q}_p$. (**Hint:** There exists an irreducible polynomial in $\mathbb{F}_p[X]$ of every degree $d \in \mathbb{N}$.)

8. For $\alpha \in \hat{\mathbb{Z}}_p$ and $n \in \mathbb{Z}_+$ define the binomial coefficient $\binom{\alpha}{n} := \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$. Show that:

(a) $\binom{\alpha}{n} \in \hat{\mathbb{Z}}_p$.

(b) The series $\sum_{n \in \mathbb{Z}_+} \binom{\alpha}{n} \beta^n$ converges in $\hat{\mathbb{Z}}_p$ for every $\beta \in \hat{\mathbb{Z}}_p$ with $|\beta|_p < 1$.