Chapter 9

Local Fields

The definition of *global field* varies in the literature, but all definitions include our primary source of examples, number fields. The other fields that are of interest in algebraic number theory are the *local fields*, which are complete with respect to a discrete valuation. This terminology will be explained as we go along.

9.1 Absolute Values and Discrete Valuations

9.1.1 Definitions and Comments

An *absolute value* on a field k is a mapping $x \to |x|$ from k to the real numbers, such that for every $x, y \in k$,
1. $|x| \geq 0$, with equality if and only if $x = 0$;
2. $|xy| = |x|\ |y|$;
3. $|x + y| \leq |x| + |y|$.

The absolute value is *nonarchimedean* if the third condition is replaced by a stronger version:
$3'$. $|x + y| \leq \max(|x|, |y|)$.
As expected, *archimedean* means not nonarchimedean.

The familiar absolute values on the reals and the complex numbers are archimedean. However, our interest will be in nonarchimedean absolute values. Here is where most of them come from.

A *discrete valuation* on k is a surjective map $v : k \to \mathbb{Z} \cup \{\infty\}$, such that for every $x, y \in k$,
(a) $v(x) = \infty$ if and only if $x = 0$;
(b) $v(xy) = v(x) + v(y)$;
(c) $v(x + y) \geq \min(v(x), v(y))$.

A discrete valuation induces a nonarchimedean absolute value via $|x| = c^{v(x)}$, where c is a constant with $0 < c < 1$.

9.1.2 Example

Let A be a Dedekind domain with fraction field K, and let P be a nonzero prime ideal of A. Then [see the proof of (4.1.6)] the localized ring A_P is a discrete valuation ring (DVR) with unique maximal ideal (equivalently, unique nonzero prime ideal) PA_P. Choose a generator π of this ideal; this is possible because a DVR is, in particular, a PID. Now if $x \in K^*$, the set of nonzero elements of K, then by factoring the principal fractional ideal $(x)A_P$, we find that $x = u\pi^n$, where $n \in \mathbb{Z}$ and u is a unit in A_P. We define $v_P(x) = n$, with $v_P(0) = \infty$. We can check that v_P is a discrete valuation, called the *P-adic valuation* on K. Surjectivity and conditions (a) and (b) follow directly from the definition. To verify (c), let $x = u\pi^m,\ y = v\pi^n$ with $m \geq n$. Then $x + y = (v^{-1}u\pi^{m-n} + 1)v\pi^n$, and since the term in parentheses belongs to A_P, the exponent in its prime factorization will be nonnegative. Therefore $v_P(x + y) \geq n = \min(v_P(x), v_P(y))$.

Now consider the special case $A = \mathbb{Z},\ K = \mathbb{Q},\ P = (p)$. If x is rational and $x = p^r a/b$ where neither a nor b is divisible by p, then we get the *p-adic valuation* on the rationals, given by $v_p(p^r a/b) = r$.

Here are some of the basic properties of nonarchimedean absolute values. It is often convenient to exclude the *trivial absolute value*, given by $|x| = 1$ for $x \neq 0$, and $|0| = 0$. Note also that for *any* absolute value, $|1| = |-1| = 1,\ |-x| = |x|$, and $|x^{-1}| = 1/|x|$ for $x \neq 0$. (Observe that $1 \times 1 = (-1) \times (-1) = x \times x^{-1} = 1$.)

9.1.3 Proposition

Let $|\ |$ be a nonarchimedean absolute value on the field K. Let A be the corresponding *valuation ring*, defined as $\{x \in K : |x| \leq 1\}$, and P the *valuation ideal* $\{x \in K : |x| < 1\}$. Then A is a local ring with unique maximal ideal P and fraction field K. If $u \in K$, then u is a unit of A if and only if $|u| = 1$. If the trivial absolute value is excluded, then A is not a field.

Proof.

1. A is a ring, because it is closed under addition, subtraction and multiplication, and contains the identity.
2. K is the fraction field of A, because if z is a nonzero element of K, then either z or its inverse belongs to A.
3. A is a local ring with unique maximal ideal P. It follows from the definition that P is a proper ideal. If Q is any proper ideal of A, then $Q \subseteq P$, because $A \setminus P \subseteq A \setminus Q$. (If $x \in A \setminus P$, then $|x| = 1$, hence $|x^{-1}| = 1$, so $x^{-1} \in A$. Thus $x \in Q$ implies that $xx^{-1} = 1 \in Q$, a contradiction.)
4. If $u \in K$, then u is a unit of A iff $|u| = 1$. For if u and v belong to A and $uv = 1$, then $|u|\ |v| = 1$. But both $|u|$ and $|v|$ are at most 1, hence they must equal 1. Conversely, if $|u| = 1$, then $|u^{-1}| = 1$. But then both u and its inverse belong to A, so u is a unit of A.
5. If $|\ |$ is nontrivial, then A is not a field. For if $x \neq 0$ and $|x| \neq 1$, then either $|x| < 1$ and $|x^{-1}| > 1$, or $|x| > 1$ and $|x^{-1}| < 1$. Either way, we have an element of A whose inverse lies outside of A. ♣

9.1.4 Proposition

If the nonarchimedean and nontrivial absolute value $|\ \ |$ on K is induced by the discrete valuation v, then the valuation ring A is a DVR.

Proof. In view of (9.1.3), we need only show that A is a PID. Choose an element $\pi \in A$ such that $v(\pi) = 1$. If x is a nonzero element of A and $v(x) = n \in \mathbb{Z}$, then $v(x\pi^{-n}) = 0$, so $x\pi^{-n}$ has absolute value 1 and is therefore a unit u by (9.1.3). Thus $x = u\pi^n$. Now if I is any proper ideal of A, then I will contain an element $u\pi^n$ with $|n|$ as small as possible, say $|n| = n_0$. Either π^{n_0} or π^{-n_0} will be a generator of I (but not both since I is proper). We conclude that every ideal of A is principal. ♣

The proof of (9.1.4) shows that A has exactly one nonzero prime ideal, namely (π).

9.1.5 Proposition

If $|\ \ |$ is a nonarchimedean absolute value , then $|x| \neq |y|$ implies $|x + y| = \max(|x|, |y|)$. Hence by induction, if $|x_1| > |x_i|$ for all $i = 2, \ldots, n$, then $|x_1 + \cdots + x_n| = |x_1|$.

Proof. We may assume without loss of generality that $|x| > |y|$. Then

$$|x| = |x + y - y| \leq \max(|x + y|, |y|) = |x + y|,$$

otherwise $\max(|x+y|, |y|) = |y| < |x|$, a contradiction. Since $|x+y| \leq \max(|x|, |y|) = |x|$, the result follows. ♣

9.1.6 Corollary

With respect to the metric induced by a nonarchimedean absolute value, all triangles are isosceles.

Proof. Let the vertices of the triangle be x, y and z. Then $|x - y| = |(x - z) + (z - y)|$. If $|x - z| = |z - y|$, then two side lengths are equal. If $|x - z| \neq |z - y|$, then by (9.1.5), $|x - y| = \max(|x - z|, |z - y|)$, and again two side lengths are equal. ♣

9.1.7 Proposition

The absolute value $|\ \ |$ is nonarchimedean if and only if $|n| \leq 1$ for every integer $n = 1 \pm \cdots \pm 1$, equivalently if and only if the set $\{|n| : n \in \mathbb{Z}\}$ is bounded.

Proof. If the absolute value is nonarchimedean, then $|n| \leq 1$ by repeated application of condition $3'$ of (9.1.1). Conversely, if every integer has absolute value at most 1, then it suffices to show that $|x + 1| \leq \max(|x|, 1)$ for every x. (Apply this result to $x/y, y \neq 0$.) By the binomial theorem,

$$|x + 1|^n = \left| \sum_{r=0}^{n} \binom{n}{r} \right| x^r \leq \sum_{r=0}^{n} \left| \binom{n}{r} \right| |x|^r.$$

By hypothesis, the integer $\binom{n}{r}$ has absolute value at most 1. If $|x| > 1$, then $|x|^r \leq |x|^n$ for all $r = 0, 1, \ldots, n$. If $|x| \leq 1$, then $|x|^r \leq 1$. Consequently,

$$|x + 1|^n \leq (n + 1) \max(|x|^n, 1).$$

Take n^{th} roots and let $n \to \infty$ to get $|x+1| \leq \max(|x|, 1)$. Finally,to show that boundedness of the set of integers is an equivalent condition, note that if $|n| > 1$, then $|n|^j \to \infty$ as $j \to \infty$ ♣

Problems For Section 9.1

1. Show that every absolute value on a finite field is trivial.
2. Show that a field that has an archimedean absolute value must have characteristic 0.
3. Two nontrivial absolute values $|\ |_1$ and $|\ |_2$ on the same field are said to be *equivalent* if for every x, $|x|_1 < 1$ if and only if $|x|_2 < 1$. [Equally well, $|x|_1 > 1$ if and only if $|x|_2 > 1$; just replace x by $1/x$ if $x \neq 0$.] This says that the absolute values induce the same topology (because they have the same sequences that converge to 0). Show that two nontrivial absolute values are equivalent if and only if for some real number a, we have $|x|_1^a = |x|_2$ for all x.

9.2 Absolute Values on the Rationals

In (9.1.2), we discussed the p-adic absolute value on the rationals (induced by the p-adic valuation, with p prime), and we are familiar with the usual absolute value. In this section, we will prove that up to equivalence (see Problem 3 of Section 9.1), there are no other nontrivial absolute values on $\mathbb{Q}$.

9.2.1 Preliminary Calculations

Fix an absolute value $|\ |$ on $\mathbb{Q}$. If m and n are positive integers greater than 1, expand m to the base n. Then $m = a_0 + a_1 n + \cdots + a_r n^r,\ 0 \leq a_i \leq n-1,\ a_r \neq 0$.

(1) $r \leq \log m / \log n$.

This follows because $n^r \leq m$.

(2) For every positive integer l we have $|l| \leq l$, hence in the above base n expansion, $|a_i| \leq a_i < n$.

This can be done by induction: $|1| = 1, |1+1| \leq |1| + |1|$, and so on.

There are $1 + r$ terms in the expansion of m, each bounded by $n[\max(1, |n|)]^r$. [We must allow for the possibility that $|n| < 1$, so that $|n|^i$ decreases as i increases. In this case, we will not be able to claim that $|a_0| \leq n(|n|^r)$.] With the aid of (1), we have

(3) $|m| \leq (1 + \log m / \log n) n [\max(1, |n|)]^{\log m / \log n}$.

Replace m by m^t and take the t^{th} root of both sides. The result is

(4) $|m| \leq (1 + t \log m / \log n)^{1/t} n^{1/t} [\max(1, |n|)]^{\log m / \log n}$.

Let $t \to \infty$ to obtain our key formula:

(5) $|m| \leq [\max(1, |n|)]^{\log m / \log n}$.

9.2.2 The Archimedean Case

Suppose that $|n| > 1$ for every $n > 1$. Then by (5), $|m| \leq |n|^{\log m/\log n}$, and therefore $\log|m| \leq (\log m/\log n)\log|n|$. Interchanging m and n gives the reverse inequality, so $\log|m| = (\log m/\log n)\log|n|$. It follows that $\log|n|/\log n$ is a constant a, so $|n| = n^a$. Since $1 < |n| \leq n$ [see (2)], we have $0 < a \leq 1$. Thus our absolute value is equivalent to the usual one.

9.2.3 The Nonarchimedean Case

Suppose that for some $n > 1$ we have $|n| \leq 1$. By (5), $|m| \leq 1$ for all $m > 1$, so $|n| \leq 1$ for all $n \geq 1$, and the absolute value is nonarchimedean by (9.1.7). Excluding the trivial absolute value, we have $|n| < 1$ for some $n > 1$. (If every nonzero integer has absolute value 1, then every nonzero rational number has absolute value 1.) Let $P = \{n \in \mathbb{Z} : |n| < 1\}$. Then P is a prime ideal (p). (Note that if ab has absolute value less than 1, so does either a or b.) Let $c = |p|$, so $0 < c < 1$.

Now let r be the exact power of p dividing n, so that p^r divides n but p^{r+1} does not. Then $n/p^r \notin P$, so $|n|/c^r = 1$, $|n| = c^r$. Note that n/p^{r+1} also fails to belong to P, but this causes no difficulty because n/p^{r+1} is not an integer.

To summarize, our absolute value agrees, up to equivalence, with the p-adic absolute value on the positive integers, hence on all rational numbers. (In going from a discrete valuation to an absolute value, we are free to choose any constant in (0,1). A different constant will yield an equivalent absolute value.)

Problems For Section 9.2

If v_p is the p-adic valuation on $\mathbb{Q}$, let $\| \ \|_p$ be the associated absolute value with the particular choice $c = 1/p$. Thus $\|p^r\|_p = p^{-r}$. Denote the usual absolute value by $\| \ \|_\infty$.

1. Establish the *product formula*: If a is a nonzero rational number, then

$$\prod_p \|a\|_p = 1$$

where p ranges over all primes, including the "infinite prime" $p = \infty$.

9.3 Artin-Whaples Approximation Theorem

The Chinese remainder theorem states that if $I_1, \ldots I_n$ are ideals in a ring R that are relatively prime in pairs, and $a_i \in I_i,\ i = 1, \ldots, n$, then there exists $a \in R$ such that $a \equiv a_i \mod I_i$ for all i. We are going to prove a result about mutually equivalent absolute values that is in a sense analogous. The condition $a \equiv a_i \mod I_i$ will be replaced by the statement that a is close to a_i with respect to the i^{th} absolute value. First, some computations.

9.3.1 Lemma

Let $|\ \ |$ be an arbitrary absolute value. Then

(1) $|a| < 1 \Rightarrow a^n \to 0$;

(2) $|a| < 1 \Rightarrow a^n/(1+a^n) \to 0$;

(3) $|a| > 1 \Rightarrow a^n/(1+a^n) \to 1$.

Proof. The first statement follows from $|a^n| = |a|^n$. To prove (2), use the triangle inequality and the observation that $1 + a^n = 1 - (-a^n)$ to get

$$1 - |a|^n \leq |1 + a^n| \leq 1 + |a|^n,$$

so by (1), $|1+a^n| \to 1$. Since $|\alpha/\beta| = |\alpha|/|\beta|$, another application of (1) gives the desired result. To prove (3), write

$$1 - \frac{a^n}{1+a^n} = \frac{1}{1+a^n} = \frac{a^{-n}}{1+a^{-n}} \to 0 \text{ by (2).} \ \clubsuit$$

Here is the key step in the development.

9.3.2 Proposition

Let $|\ \ |_1, \ldots, |\ \ |_n$ be nontrivial, mutually inequivalent absolute values on the same field. Then there is an element a such that $|a|_1 > 1$ and $|a|_i < 1$ for $i = 2, \ldots, n$.

Proof. First consider the case $n = 2$. Since $|\ \ |_1$ and $|\ \ |_2$ are inequivalent, there are elements b and c such that $|b|_1 < 1,\ |b|_2 \geq 1,\ |c|_1 \geq 1,\ |c|_2 < 1$. If $a = c/b$, then $|a|_1 > 1$ and $|a|_2 < 1$.

Now if the result holds for $n-1$, we can choose an element b such that $|b|_1 > 1, |b|_2 < 1, \ldots, |b|_{n-1} < 1$. By the $n = 2$ case, we can choose c such that $|c|_1 > 1$ and $|c|_n < 1$.

Case 1. Suppose $|b|_n \leq 1$. Take $a_r = cb^r,\ r \geq 1$. Then $|a_r|_1 > 1,\ |a_r|_n < 1$, and $|a_r|_i \to 0$ as $r \to \infty$ for $i = 2, \ldots, n-1$. Thus we can take $a = a_r$ for sufficiently large r.

Case 2. Suppose $|b|_n > 1$. Take $a_r = cb^r/(1+b^r)$. By (3) of (9.3.1), $|a_r|_1 \to |c|_1 > 1$ and $|a_r|_n \to |c|_n < 1$ as $r \to \infty$. If $2 \leq i \leq n-1$, then $|b|_i < 1$, so by (2) of (9.3.1), $|a_r|_i \to 0$ as $r \to \infty$. Again we can take $a = a_r$ for sufficiently large r. $\clubsuit$

9.3.3 Approximation Theorem

Let $|\ \ |_1, \ldots, |\ \ |_n$ be nontrivial mutually inequivalent absolute values on the field k. Given arbitrary elements $x_1, \ldots, x_n \in k$ and any positive real number ϵ, there is an element $x \in k$ such that $|x - x_i|_i < \epsilon$ for all $i = 1, \ldots, n$.

Proof. By (9.3.2), $\forall i\ \exists y_i \in k$ such that $|y_i|_i > 1$ and $|y_i|_j < 1$ for $j \neq i$. Take $z_i = y_i^r/(1+y_i^r)$. Given $\delta > 0$, it follows from (2) and (3) of (9.3.1) that for r sufficiently large,

$$|z_i - 1|_i < \delta \text{ and } |z_j| < \delta,\ j \neq i.$$

Our candidate is

$$x = x_1 z_1 + \cdots x_n z_n.$$

To show that x works, note that $x - x_i = \sum_{j \neq i} x_j z_j + x_i(z_i - 1)$. Thus

$$|x - x_i|_i \leq \delta \sum_{j \neq i} |x_j|_i + \delta |x_i|_i = \delta \sum_{j=1}^{n} |x_j|_i \ .$$

Choose δ so that the right side is less than ϵ, and the result follows. ♣

Problems For Section 9.3

1. Let $|\ \ |_1, \ldots, |\ \ |_n$ be nontrivial mutually inequivalent absolute values on the field k. Fix r with $0 \leq r \leq n$. Show that there is an element $a \in k$ such that $|a|_1 > 1, \ldots, |a|_r > 1$ and $|a|_{r+1}, \ldots, |a|_n < 1$.
2. There is a gap in the first paragraph of the proof of (9.3.2), which can be repaired by showing that the implication $|a|_1 < 1 \Rightarrow |a|_2 < 1$ is sufficient for equivalence. Prove this.

9.4 Completions

You have probably seen the construction of the real numbers from the rationals, and the general process of completing a metric space using equivalence classes of Cauchy sequences. If the metric is induced by an absolute value on a field, then we have some additional structure that we can exploit to simplify the development. If we complete the rationals with respect to the p-adic rather than the usual absolute value, we get the p-adic numbers, the most popular example of a local field.

9.4.1 Definitions and Comments

Let K be a field with an absolute value $|\ \ |$, and let C be the set of Cauchy sequences with elements in K. Then C is a ring under componentwise addition and multiplication. Let N be the set of *null sequences* (sequences converging to 0). Then N is an ideal of C (because every Cauchy sequence is bounded). In fact N is a maximal ideal, because every Cauchy sequence not in N is eventually bounded away from 0, hence is a unit in C. The *completion* of K with respect to the given absolute value is the field $\hat{K} = C/N$. We can embed K in $\hat{K}$ via $c \to \{c, c, \ldots\} + N$.

We now extend the absolute value on K to $\hat{K}$. If $(c_n) + N \in \hat{K}$, then $(|c_n|)$ is a Cauchy sequence of real numbers, because by the triangle inequality, $|c_n| - |c_m|$ has (ordinary) absolute value at most $|c_n - c_m| \to 0$ as $n, m \to \infty$. Thus $|c_n|$ converges to a limit, which we take as the absolute value of $(c_n) + N$. Since the original absolute value satisfies the defining conditions in (9.1.1), so does the extension.

To simplify the notation, we will denote the element $(c_n) + N$ of $\hat{K}$ by (c_n). If $c_n = c \in K$ for all n, we will write the element as c.

9.4.2 Theorem

K is dense in $\hat{K}$ and $\hat{K}$ is complete.

Proof. Let $\alpha = (c_n) \in \hat{K}$, with $\alpha_n = c_n$. Then

$$|\alpha - \alpha_n| = \lim_{m\to\infty} |c_m - c_n| \to 0 \text{ as } n \to \infty,$$

proving that K is dense in $\hat{K}$. To prove completeness of $\hat{K}$, let (α_n) be a Cauchy sequence in $\hat{K}$. Since K is dense, for every positive integer n there exists $c_n \in K$ such that $|\alpha_n - c_n| < 1/n$. But then (c_n) is a Cauchy sequence in $\hat{K}$, hence in K, and we are assured that $\alpha = (c_n)$ is a legal element of $\hat{K}$. Moreover, $|\alpha_n - \alpha| \to 0$, proving completeness. ♣

9.4.3 Uniqueness of the Completion

Suppose K is isomorphic to a dense subfield of the complete field L, where the absolute value on L extends that of (the isomorphic copy of) K. If $x \in \hat{K}$, then there is a sequence $x_n \in K$ such that $x_n \to x$. But the sequence (x_n) is also Cauchy in L, hence converges to an element $y \in L$. If we define $f(x) = y$, then f is a well-defined homomorphism of fields, necessarily injective. If $y \in L$, then y is the limit of a Cauchy sequence in K, which converges to some $x \in \hat{K}$. Consequently, $f(x) = y$. Thus f is an isomorphism of $\hat{K}$ and L, and f preserves the absolute value.

9.4.4 Power Series Representation

We define a *local field* K as follows. There is an absolute value on K induced by a discrete valuation v, and with respect to this absolute value, K is complete. For short, we say that K is complete with respect to the discrete valuation v. Let A be the valuation ring (a DVR), and P the valuation ideal; see (9.1.3) and (9.1.4) for terminology. If $\alpha \in K$, then by (9.1.4) we can write $\alpha = u\pi^r$ with $r \in \mathbb{Z}, u$ a unit in A and π an element of A such that $v(\pi) = 1$. Often, π is called a *prime element* or a *uniformizer*. Note that $A = \{\alpha \in K : v(\alpha) \geq 0\}$ and $P = \{\alpha \in K : v(\alpha) \geq 1\} = A\pi$.

Let S be a fixed set of representatives of the cosets of A/P. We will show that each $\alpha \in K$ has a Laurent series expansion

$$\alpha = a_{-m}\pi^{-m} + \cdots + a_{-1}\pi^{-1} + a_0 + a_1\pi + a_2\pi^2 + \cdots, a_i \in S,$$

and if a_r is the first nonzero coefficient (r may be negative), then $v(\alpha) = r$.

The idea is to expand the unit u in a power series involving only nonnegative powers of π. For some $a_0 \in S$ we have $u - a_0 \in P$. But then $v(u - a_0) \geq 1$, hence $v((u - a_0)/\pi) \geq 0$, so $(u - a_0)/\pi \in A$. Then for some $a_1 \in S$ we have $[(u - a_0)/\pi] - a_1 \in P$, in other words,

$$\frac{u - a_0 - a_1\pi}{\pi} \in P.$$

Repeating the above argument, we get

$$\frac{u - a_0 - a_1\pi}{\pi^2} \in A.$$

Continue inductively to obtain the desired series expansion. Note that by definition of S, the coefficients a_i are unique. Thus an expansion of α that begins with a term of degree r in π corresponds to a representation $\alpha = u\pi^r$ and a valuation $v(\alpha) = r$. Also, since $|\pi| < 1$, high positive powers of π are small with respect to the given absolute value. The partial sums s_n of the series form a *coherent sequence*, that is, $s_n \equiv s_{n-1} \mod (\pi)^n$.

9.4.5 Proposition

Let $\sum a_n$ be any series of elements in a local field. Then the series converges if and only if $a_n \to 0$.

Proof. If the series converges, then $a_n \to 0$ by the standard calculus argument, so assume that $a_n \to 0$. Since the absolute value is nonarchimedean, $n \leq m$ implies that

$$|\sum_{i=n}^{m} a_i| \leq \max(a_n, \ldots, a_m) \to 0 \text{ as } n \to \infty. \ \clubsuit$$

9.4.6 Definitions and Comments

The completion of the rationals with respect to the p-adic valuation is called the field of *p-adic numbers*, denoted by $\mathbb{Q}_p$. The valuation ring $A = \{\alpha : v(\alpha) \geq 0\}$ is called the ring of *p-adic integers*, denoted by $\mathbb{Z}_p$. The series representation of a p-adic integer contains only nonnegative powers of $\pi = p$. If in addition, there is no constant term, we get the valuation ideal $P = \{\alpha : v(\alpha) \geq 1\}$. The set S of coset representatives may be chosen to be $\{0, 1, \ldots, p-1\}$. (Note that if $a \neq b$ and $a \equiv b \mod p$, then $a - b \in P$, so a and b cannot both belong to S. Also, a rational number can always be replaced by an integer with the same valuation.) Arithmetic is carried out via polynomial multiplication, except that there is a "carry". For example, if $p = 7$, then $3 + 6 = 9 = 2 + p$. For some practice, see the exercises.

We adopt the convention that in going from the p-adic valuation to the associated absolute value $|x| = c^{v(x)}, 0 < c < 1$, we take $c = 1/p$. Thus $|p^r| = p^{-r}$.

Problems For Section 9.4

1. Show that a rational number a/b (in lowest terms) is a p-adic integer if and only if p does not divide b.
2. With $p = 3$, express the product of $(2 + p + p^2)$ and $(2 + p^2)$ as a p-adic integer.
3. Express the p-adic integer -1 as an infinite series.
4. Show that the sequence $a_n = n!$ of p-adic integers converges to 0.
5. Does the sequence $a_n = n$ of p-adic integers converge?
6. Show that the p-adic power series for $\log(1+x)$, namely $\sum_{n=1}^{\infty}(-1)^{n+1}x^n/n$, converges in $\mathbb{Q}_p$ for $|x| < 1$ and diverges elsewhere. This allows a definition of a p-adic logarithm: $\log_p(x) = \log[1 + (x - 1)]$.

In Problems 7-9, we consider the p-adic exponential function.

7. Recall from elementary number theory that the highest power of p dividing $n!$ is $\sum_{i=1}^{\infty}\lfloor n/p^i \rfloor$. (As an example, let $n = 15$ and $p = 2$. Calculate the number of multiples of 2, 4,and 8 in the integers 1-15.) Use this result to show that the p-adic valuation of $n!$ is at most $n/(p-1)$.
8. Show that the p-adic valuation of $(p^m)!$ is $(p^m - 1)/(p - 1)$.
9. Show that the exponential series $\sum_{n=0}^{\infty} x^n/n!$ converges for $|x| < p^{-1/(p-1)}$ and diverges elsewhere.

9.5 Hensel's Lemma

9.5.1 The Setup

Let K be a local field with valuation ring A and valuation ideal P. By (9.1.3) and (9.1.4), A is a local ring, in fact a DVR, with maximal ideal P. The field $k = A/P$ is called the *residue field* of A or of K. If $a \in A$, then the coset $a + P \in k$ will be denoted by $\overline{a}$. If f is a polynomial in $A[X]$, then reduction of the coefficients of f mod P yields a polynomial $\overline{f}$ in $k[X]$. Thus

$$f(X) = \sum_{i=0}^{d} a_i X^i \in A[X],\ \overline{f}(X) = \sum_{i=0}^{d} \overline{a}_i X^i \in k[X].$$

Hensel's lemma is about lifting a factorization of $\overline{f}$ from $k[X]$ to $A[X]$. Here is the precise statement.

9.5.2 Hensel's Lemma

Assume that f is a monic polynomial of degree d in $A[X]$, and that the corresponding polynomial $F = \overline{f}$ factors as the product of relatively prime monic polynomials G and H in $k[X]$. Then there are monic polynomials g and h in $A[X]$ such that $\overline{g} = G,\ \overline{h} = H$ and $f = gh$.

Proof. Let r be the degree of G, so that $\deg H = d - r$. We will inductively construct $g_n, h_n \in A[X], n = 1, 2, \ldots$, such that $\deg g_n = r,\ \deg h_n = d - r,\ \overline{g}_n = G,\ \overline{h}_n = H$, and

$$f(X) - g_n(X)h_n(X) \in P^n[X].$$

Thus the coefficients of $f - g_n h_n$ belong to P^n.

The basis step: Let $n = 1$. Choose monic $g_1, h_1 \in A[X]$ such that $\overline{g}_1 = G$ and $\overline{h}_1 = H$. Then $\deg g_1 = r$ and $\deg h_1 = d - r$. Since $\overline{f} = \overline{g}_1 \overline{h}_1$, we have $f - g_1 h_1 \in P[X]$.

The inductive step: Assume that g_n and h_n have been constructed. Let $f(X) - g_n(X)h_n(X) = \sum_{i=0}^{d} c_i X^i$ with the $c_i \in P^n$. Since $G = \overline{g}_n$ and $H = \overline{h}_n$ are relatively prime, for each $i = 0, \ldots, d$ there are polynomials $\overline{v}_i$ and $\overline{w}_i$ in $k[X]$ such that

$$X^i = \overline{v}_i(X)\overline{g}_n(X) + \overline{w}_i(X)\overline{h}_n(X).$$

Since $\overline{g}_n$ has degree r, the degree of $\overline{v}_i$ is at most $d - r$, and similarly the degree of $\overline{w}_i$ is at most r. Moreover,

$$X^i - v_i(X)g_n(X) - w_i(X)h_n(X) \in P[X]. \qquad (1)$$

We define

$$g_{n+1}(X) = g_n(X) + \sum_{i=0}^{d} c_i w_i(X),\ h_{n+1}(X) = h_n(X) + \sum_{i=0}^{d} c_i v_i(X).$$

Since the c_i belong to $P^n \subseteq P$, it follows that $\overline{g}_{n+1} = \overline{g}_n = G$ and $\overline{h}_{n+1} = \overline{h}_n = H$. Since the degree of g_{n+1} is at most r, it must be exactly r, and similarly the degree of h_{n+1} is $d - r$. To check the remaining condition,

$$f - g_{n+1}h_{n+1} = f - (g_n + \sum_i c_i w_i)(h_n + \sum_i c_i v_i)$$

$$= (f - g_n h_n - \sum_i c_i X^i) + \sum_i c_i (X^i - g_n v_i - h_n w_i) - \sum_{i,j} c_i c_j w_i v_j.$$

By the induction hypothesis, the first grouped term on the right is zero, and, with the aid of Equation (1) above, the second grouped term belongs to $P^n P[X] = P^{n+1}[X]$. The final term belongs to $P^{2n}[X] \subseteq P^{n+1}[X]$, completing the induction.

Finishing the proof. By definition of g_{n+1}, we have $g_{n+1} - g_n \in P^n[X]$, so for any fixed i, the sequence of coefficients of X^i in $g_n(X)$ is Cauchy and therefore converges. To simplify the notation we write $g_n(X) \to g(X)$, and similarly $h_n(X) \to h(X)$, with $g(X), h(X) \in A[X]$. By construction, $f - g_n h_n \in P^n[X]$, and we may let $n \to \infty$ to get $f = gh$. Since $\overline{g}_n = G$ and $\overline{h}_n = H$ for all n, we must have $\overline{g} = G$ and $\overline{h} = H$. Since f, G and H are monic, the highest degree terms of g and h are of the form $(1+a)X^r$ and $(1+a)^{-1}X^{d-r}$ respectively, with $a \in P$. (Note that $1 + a$ must reduce to 1 mod P.) By replacing g and h by $(1+a)^{-1}g$ and $(1+a)h$, respectively, we can make g and h monic without disturbing the other conditions. The proof is complete. ♣

9.5.3 Corollary

With notation as in (9.5.1), let f be a monic polynomial in $A[X]$ such that $\overline{f}$ has a simple root $\eta \in k$. Then f has a simple root $a \in A$ such that $\overline{a} = \eta$.

Proof. We may write $\overline{f}(X) = (X - \eta)H(X)$ where $X - \eta$ and $H(X)$ are relatively prime in $k[X]$. By Hensel's lemma, we may lift the factorization to $f(X) = (X - a)h(X)$ with $h \in A[X], a \in A$ and $\overline{a} = \eta$. If a is a multiple root of f, then η is a multiple root of $\overline{f}$, which is a contradiction. ♣

Problems For Section 9.5

1. Show that for any prime p, there are $p - 1$ distinct $(p-1)^{\text{th}}$ roots of unity in $\mathbb{Z}_p$.
2. Let p be an odd prime not dividing the integer m. We wish to determine whether m is a square in $\mathbb{Z}_p$. Describe an effective procedure for doing this.
3. In Problem 2, suppose that we not only want to decide if m is a square in $\mathbb{Z}_p$, but to find the series representation of $\sqrt{m}$ explicitly. Indicate how to do this, and illustrate with an example.