18.782 Introduction to Arithmetic Geometry **Fall 2013**
Lecture #4 **09/17/2013**

4.1 Inverse limits

Definition 4.1. An *inverse system* is a sequence of objects (e.g. sets/groups/rings) (A_n) together with a sequence of morphisms (e.g. functions/homomorphisms) (f_n)

$$\cdots \longrightarrow A_{n+1} \xrightarrow{f_n} A_n \longrightarrow \cdots \longrightarrow A_2 \xrightarrow{f_1} A_1.$$

The *inverse limit*

$$A = \varprojlim A_n$$

is the subset of the direct product $\prod_n A_n$ consisting of those sequences $a = (a_n)$ for which $f_n(a_{n+1}) = a_n$ for all $n \geq 1$. For each $n \geq 1$ the *projection map* $\pi_n \colon A \to A_n$ sends a to a_n.

Remark 4.2. For those familiar with category theory, one can define inverse limits for any category. In most cases the result will be another object of the same category (unique up to isomorphism), in which case the projection maps are then morphisms in that category. We will restrict our attention to the familiar categories of sets, groups, and rings. One can also generalize the index set $\{n\}$ from the positive integers to any partially ordered set.

4.2 The ring of p-adic integers

Definition 4.3. For a prime p, the *ring of p-adic integers* $\mathbb{Z}_p$ is the inverse limit

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

of the inverse system of rings $(\mathbb{Z}/p^n\mathbb{Z})$ with morphisms (f_n) given by reduction modulo p^n (for a residue class $\overline{x} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$, pick an integer $x \in \overline{x}$ and take its residue class in $\mathbb{Z}/p^n\mathbb{Z}$).

The multiplicative identity in $\mathbb{Z}_p$ is $1 = (\bar{1}, \bar{1}, \bar{1}, \ldots)$, where the nth $\bar{1}$ denotes the residue class of 1 in $\mathbb{Z}/p^n\mathbb{Z}$. The map that sends each integer $x \in \mathbb{Z}$ to the sequence $(\bar{x}, \bar{x}, \bar{x}, \ldots)$ is a ring homomorphism, and its kernel is clearly trivial, since 0 is the only integer congruent to $0 \bmod p^n$ for all n. Thus the ring $\mathbb{Z}_p$ has characteristic 0 and contains $\mathbb{Z}$ as a subring. But $\mathbb{Z}_p$ is a much bigger ring than $\mathbb{Z}$.

Example 4.4. If we represent elements of $\mathbb{Z}/p^n\mathbb{Z}$ by integers in $[0, p^n - 1]$, in $\mathbb{Z}_7$ we have

$$\begin{aligned}
2 &= (2, 2, 2, 2, 2, \ldots)\\
2002 &= (0, 42, 287, 2002, 2002, \ldots)\\
-2 &= (5, 47, 341, 2399, 16805, \ldots)\\
2^{-1} &= (4, 25, 172, 1201, 8404, \ldots)\\
\sqrt{2} &= \begin{cases} (3, 10, 108, 2166, 4567 \ldots)\\ (4, 39, 235, 235, 12240 \ldots)\end{cases}\\
\sqrt[5]{2} &= (4, 46, 95, 1124, 15530, \ldots)
\end{aligned}$$

Note that 2002 is not invertible in $\mathbb{Z}_7$, and that while 2 has two square roots in $\mathbb{Z}_7$, it has only one fifth root, and no cube roots.

Andrew V. Sutherland

While representing elements of $\mathbb{Z}_p$ as sequences (a_n) with $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ follows naturally from the definition of $\mathbb{Z}_p$ as an inverse limit, it is redundant. The value of a_n constrains the value of a_{n+1} to just p of the p^{n+1} elements of $\mathbb{Z}/p^{n+1}\mathbb{Z}$, namely, those that are congruent to a_n modulo p^n. If we uniquely represent each a_n as an integer in the interval $[0, p^n - 1]$ we can always write $a_{n+1} = a_n + p^n b_n$ with $b_n \in [0, p-1]$.

Definition 4.5. Let $a = (a_n)$ be a p-adic integer with each a_n uniquely represented by an integer in $\in [0, p^n - 1]$. The sequence $(b_0, b_1, b_2, \ldots)$ with $b_0 = a_1$ and $b_n = (a_{n+1} - a_n)/p^n$ is called the *p-adic expansion of a*.

Theorem 4.6. *Every element of $\mathbb{Z}_p$ has a unique p-adic expansion and every sequence $(b_0, b_1, b_2, \ldots)$ of integers in $[0, p-1]$ is the p-adic expansion of an element of $\mathbb{Z}_p$.*

Proof. This follows immediately from the definition: we can recover (a_n) from its p-adic expansion $(b_0, b_1, b_2, \ldots)$ via $a_1 = a_0$ and $a_{n+1} = a_n + pb_n$ for all $n \geq 1$. □

Thus we have a bijection between $\mathbb{Z}_p$ and the set of all sequences of integers in $[0, p-1]$ indexed by the nonnegative integers.

Example 4.7. We have the following p-adic expansion in $\mathbb{Z}_7$:

$$\begin{aligned}
2 &= (2, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots) \\
2002 &= (0, 6, 5, 5, 0, 0, 0, 0, 0, 0, \ldots) \\
-2 &= (5, 6, 6, 6, 6, 6, 6, 6, 6, 6, \ldots) \\
2^{-1} &= (4, 3, 3, 3, 3, 3, 3, 3, 3, 3, \ldots) \\
5^{-1} &= (3, 1, 4, 5, 2, 1, 4, 5, 2, 1, \ldots) \\
\sqrt{2} &= \begin{cases} (3, 1, 2, 6, 1, 2, 1, 2, 4, 6 \ldots) \\ (4, 5, 4, 0, 5, 4, 5, 4, 2, 0 \ldots) \end{cases} \\
\sqrt[5]{2} &= (4, 6, 1, 3, 6, 4, 3, 5, 4, 6 \ldots)
\end{aligned}$$

You can easily recreate these examples (and many more) in Sage. To create the ring of 7-adic integers, just type `Zp(7)`. By default Sage will use 20 digits of p-adic precision, but you can change this to n digits using `Zp(p,n)`.

Performing arithmetic in $\mathbb{Z}_p$ using p-adic expansions is straight-forward. One computes a sum of p-adic expansions $(b_0, b_1, \ldots) + (c_0, c_1, \ldots)$ by adding digits mod p and carrying to the right (don't forget to carry!). Multiplication corresponds to computing products of formal power series in p, e.g. $\left(\sum b_n p^n\right)\left(\sum c_n p^n\right)$, and can be performed by hand using the standard schoolbook algorithm for multiplying integers represented in base 10, except now one works in base p. But Sage will do happily do all this arithmetic for you; I encourage you to experiment in Sage in order to build your intuition.

4.3 Properties of $\mathbb{Z}_p$

Recall that a sequence of group homomorphisms is *exact* if, for each intermediate group in the sequence, the image of the incoming homomorphism is equal to the kernel of the outgoing homomorphism. In the case of a *short exact sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

this simply means that f is injective, g is surjective, and $\operatorname{im} f = \ker g$. In this situation the the homomorphism g induces an isomorphism $B/f(A) \simeq C$.

Theorem 4.8. *For each positive integer m, the sequence*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{[p^m]} \mathbb{Z}_p \xrightarrow{\pi_m} \mathbb{Z}/p^m\mathbb{Z} \longrightarrow 0,$$

is exact. Here $[p^m]$ is the multiplication-by-p^m map and π_m is the projection to $\mathbb{Z}/p^m\mathbb{Z}$.

Proof. The map $[p^m]$ shifts the p-adic expansion $(b_0, b_1, \ldots)$ of each element in $\mathbb{Z}_p$ to the right by m digits (filling with zeroes) yielding

$$(c_0, c_1, c_2, \ldots) = (0, \ldots, 0, b_0, b_1, b_2, \ldots),$$

with $c_n = 0$ for $n < m$ and $c_n = b_{n-m}$ for all $n \geq m$. This is clearly an injective operation on p-adic expansions, and hence on $\mathbb{Z}_p$, and the image of $[p^m]$ consists of the elements in $\mathbb{Z}_p$ whose p-adic expansion $(c_0, c_1, c_2, \ldots)$ satisfies $c_0 = \cdots = c_{m-1} = 0$.

Conversely, the map π_m sends the p-adic expansion $(b_0, b_1, b_2, \ldots,)$ to the sum

$$b_0 + b_1 p + b_2 p^2 + \cdots b_{m-1} p^{m-1}$$

in $\mathbb{Z}/p^m\mathbb{Z}$. Each element of $\mathbb{Z}/p^m\mathbb{Z}$ is uniquely represented by an integer in $[0, p^m - 1]$, each of which can be (uniquely) represented by a sum as above, with $b_0, \ldots, b_{m-1}$ integers in $[0, p-1]$. It follows that π_m is surjective, and its kernel consists of the elements in $\mathbb{Z}_p$ whose p-adic expansion $(b_0, b_1, b_2, \ldots)$ satisfies $b_0 = \cdots = b_{m-1} = 0$, which is precisely $\operatorname{im}[p^m]$. □

Corollary 4.9. *For all positive integers m we have $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$.*

Definition 4.10. For each nonzero $a \in \mathbb{Z}_p$ the *p-adic valuation* of a, denoted $v_p(a)$, is the greatest integer m for which a lies in the image of $[p^m]$; equivalently, $v_p(a)$ is the index of the first nonzero entry in the p-adic expansion of a. We also define $v_p(0) = \infty$, and adopt the conventions that $n < \infty$ and $n + \infty = \infty$ for any integer n.

Theorem 4.11. *The p-adic valuation v_p satisfies the following properties:*

(1) $v_p(a) = \infty$ *if and only if* $a = 0$.

(2) $v_p(ab) = v_p(a) + v_p(b)$.

(3) $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Proof. The first property is immediate from the definition. The second two are clear when either a or b is zero, so we assume otherwise and let $m = v_p(a)$ and $n = v_p(b)$.

For (2) we have $a = p^m a'$ and $b = p^n b'$, for some $a', b' \in \mathbb{Z}_p$, and therefore $ab = p^{m+n} a'b'$ lies in $\operatorname{im}[p^{m+n}]$ and $v_p(ab) \geq m + n$. On the other hand, the coefficient of p^m in the p-adic expansion of a and the coefficient of p^n in the p-adic expansion of b are both nonzero, so the coefficient of p^{m+n} in the p-adic expansion of ab is nonzero, thus $v_p(ab) \leq m + n$.

For (3) we assume without loss of generality that $m \leq n$, in which case $\operatorname{im}[p^n] \subseteq \operatorname{im}[p^m]$, so a and b both lie in $\operatorname{im}[p^m]$, as does $a+b$, and we have $v_p(a+b) \geq m = \min(v_p(a), v_p(b))$. □

The p-adic valuation v_p is an example of a *discrete valuation.*

Definition 4.12. Let R be a commutative ring. A *discrete valuation* (on R) is a function $v\colon R \to \mathbb{Z} \bigcup \{\infty\}$ that satisfies the three properties listed in Theorem 4.11.

Corollary 4.13. *$\mathbb{Z}_p$ is an integral domain (a ring with no zero divisors).*

Proof. If a and b are both nonzero then $v_p(ab) = v_p(a) + v_p(b) < \infty$, so $ab \neq 0$. □

Definition 4.14. The group of *p-adic units* $\mathbb{Z}_p^\times$ is the multiplicative group of invertible elements in $\mathbb{Z}_p$.

Theorem 4.15. *The following hold:*

(1) $\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p$; equivalently, $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p : v_p(a) = 0\}$.

(2) Every nonzero $a \in \mathbb{Z}_p$ can be uniquely written as $p^n u$ with $n \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^\times$.

Proof. We first note $v_p(p^m) = m$ for all $m \geq 0$, and in particular, $v_p(1) = 0$. If $a \in \mathbb{Z}_p^\times$, then a has a multiplicative inverse a^{-1} and we have $v_p(a) + v_p(a^{-1}) = v_p(1) = 0$, which implies that $v_p(a) = v_p(a^{-1}) = 0$, since $v_p(a)$ is nonnegative for all $a \in \mathbb{Z}_p$. Conversely, if $a = (a_n)$ with each $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ and $v_p(a) = 0$, then $a_1 \not\equiv 0 \bmod p$ is invertible in $\mathbb{Z}/p\mathbb{Z}$, and since $a_n \equiv a_1 \not\equiv 0 \bmod p$, each a_n is invertible in $\mathbb{Z}/p^n\mathbb{Z}$. So $a^{-1} = (a_n^{-1}) \in \mathbb{Z}_p$, which proves (1).

For (2), if $a \in \mathbb{Z}_p$ is nonzero, let $v_p(a) = m$. Then $a \in \operatorname{im}[p^m]$ and therefore $a = p^m u$ for some $u \in \mathbb{Z}_p$. We then have

$$m = v_p(a) = v_p(p^m u) = v_p(p^m) + v_p(u) = m + v_p(u),$$

so $v_p(u) = 0$, and therefore $u \in \mathbb{Z}_p^\times$. □

Theorem 4.16. *Every nonzero ideal in $\mathbb{Z}_p$ is of the form (p^m) for some integer $m \geq 0$.*

Proof. Let I be a nonzero ideal in $\mathbb{Z}_p$, and let $m = \inf\{v_p(a) : a \in I\}$. Then $m < \infty$ (since I is nonzero), and every $a \in I$ lies in $\operatorname{im}[p^m] = (p^m)$. On the other hand, $v_p(a) = m$ for some $a \in I$ (since v_p is discrete), and we can write $a = p^m u$ for some unit u. But then $u^{-1}a = p^m \in I$ (since I is closed under multiplication by elements of R), thus $p^m \in I \subseteq (p^m)$ which implies $I = (p^m)$. □

Corollary 4.17. *The ring $\mathbb{Z}_p$ is a principal ideal domain with a unique maximal ideal.*

Definition 4.18. A *discrete valuation ring* is a principal ideal domain which contains a unique maximal ideal and is not a field.

This definition of a discrete valuation ring might seem strange at first glance, since it doesn't mention a valuation. But given a discrete valuation ring R with maximal ideal (p), where p is any irreducible element of R, we can define $v\colon R \to \mathbb{Z} \bigcup \{\infty\}$ by setting $v(0) = \infty$ and for every nonzero $a \in R$ defining $v(a)$ as the greatest positive integer n for which $a \in (p^n)$. It is then easy to check that v is a discrete valuation on R.

Discrete valuation rings are about as close as a commutative ring can get to being a field without actually becoming one. To turn a discrete valuation ring into a field, we only need to invert one element (any generator for its maximal ideal). Another remarkable fact about discrete valuation rings is that (up to units) they are unique factorization domains with exactly one prime!