27. l-ADIC INTEGERS (CONTINUED)

Recall (last time): If $A = \mathbb{Z}$, $l \geq 2$ an integer and $I = (l)$, the associated completion $\widehat{A}_I$ is denoted by $\widehat{\mathbb{Z}}_l$ and called the ring of l-adic integers.

Theorem 27.1. *The following hold:*

(a) *If p is a prime, then $\widehat{\mathbb{Z}}_p$ is a domain and also a local ring (which is not a field)*
(b) *If $l = p^\alpha$ is a prime power, then $\widehat{\mathbb{Z}}_p \cong \widehat{\mathbb{Z}}_l$*
(c) *In general, if $l = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where $p_1, \dots, p_k$ are distinct primes, then*

$$\widehat{\mathbb{Z}}_l \cong \widehat{\mathbb{Z}}_{p_1} \times \dots \times \widehat{\mathbb{Z}}_{p_k}.$$

Remark: (c) implies that $\widehat{\mathbb{Z}}_l$ is not a domain if l is not a prime power.

Proof. (a) Let $R = \widehat{\mathbb{Z}}_p$. By Claim 26.1(2) any $a \in R$ can be uniquely written as $a = a_0 + a_1 p + a_2 p^2 + \dots$ where $0 \leq a_i \leq p-1$.
Let $M = pR$. Note that $a \in M \iff a_0 = 0$. Clearly, M is an ideal of R and $M \neq R$. We will show that any element of $R \setminus M$ is a unit. This will imply that R is a local ring with maximal ideal M (and R is not a field since $M \neq 0$).
Take $a \in R \setminus M$, so that $a_0 \neq 0$.
Case 1: $a_0 = 1$. In this case $a = 1 + pb$ for some $b \in R$. Direct verification shows that the element $1 - pb + (pb)^2 - (pb)^3 + \dots$ is the inverse of a. Note that this power series is convergent by Claim 26.1(1).
Case 2: $1 < a_0 < p$. Choose $k \in \mathbb{Z}$ such that $a_0 k = 1 + pc$ for some $c \in \mathbb{Z}$. We know that $a = a_0 + pb$, so $ka = ka_0 + pkb = 1 + p(c + kb)$ is a unit by case 1. Since ka is a unit, a must also be a unit.
It remains to prove that R is a domain. Suppose not and there exist nonzero $a, b \in R$ such that $ab = 0$. We know that $a = a_m p^m + a_{m+1} p^{m+1} + \dots$ and $b = b_k p^k + b_{k+1} p^{k+1} + \dots$ for some $m, k \in \mathbb{Z}_{\geq 0}$ where $a_m, b_k \neq 0$. But then

$$0 = ab = p^{m+k}(a_m + pa_{m+1} + \dots)(b_k + pb_{k+1} + \dots)$$

As we just proved the elements $a_m + pa_{m+1} + \dots$ and $b_k + pb_{k+1} + \dots$ are both units, so the above equality implies that $p^{m+k} = 0$ which is clearly false. This finishes the proof of (a).

(b) is a special case of the following general result:

Fact. *Let A be a ring, I an ideal of A with $\bigcap_n I^n = \{0\}$, and $J = I^m$ for some $m \in \mathbb{N}$. Then the I-adic and J-adic metrics on A induce the same topology, and thus $\widehat{A}_I \cong \widehat{A}_J$.*

This claim, in turn, easily follows from the definition of I-adic topology.

Finally, part (c) is proved using the Chinese Remainder Theorem. In order to give a rigorous argument we need the notion of an inverse limit. □

27.1. **Inverse limits (easy case).** Suppose that we are given a sequence of rings $A_1, A_2, \ldots$ and homomorphisms $\pi_n : A_{n+1} \to A_n$ for each $n \in \mathbb{N}$. We will say that

$$A_1 \xleftarrow{\pi_1} A_2 \xleftarrow{\pi_2} A_3 \xleftarrow{\pi_3} \ldots$$

is an inverse system of rings. The inverse limit $\varprojlim_{n\in\mathbb{N}} A_n$ is defined to be the following subset o $\prod_{n=1}^{\infty} A_n$:

$$\varprojlim_{n\in\mathbb{N}} A_n = \{(a_1, a_2, \ldots) \in \prod A_n \,:\, \pi_n(a_{n+1}) = a_n \text{ for all } n \in \mathbb{N}\}.$$

It is easy to see that $\varprojlim_{n\in\mathbb{N}} A_n$ is in fact a subring of $\prod A_n$.

Theorem 27.2 (Connection between inverse limits and completions)**.** *Let A be a ring and I an ideal of A with $\bigcap_{n\in\mathbb{N}} I^n = \{0\}$. Consider the inverse system of rings*

$$A/I \xleftarrow{\pi_1} A/I^2 \xleftarrow{\pi_2} \ldots$$

where each π_i is a natural surjection. Then $\varprojlim_{n\in\mathbb{N}} A/I^n \cong \widehat{A}_I$ as rings.

Proof (sketch). Take $x \in \varprojlim A/I^n$. By definition $x = (a_1 + I, a_2 + I^2, \ldots)$ where $\pi_n(a_{n+1}+I^{n+1}) = a_n+I^n$ for each n. On the other hand, by definition of natural projections $\pi_n(a_{n+1} + I^{n+1}) = a_{n+1} + I^n$. Thus, $a_{n+1} - a_n \in I^n$. For any $m > n$ we have $a_m - a_n = \sum_{i=n}^{m-1}(a_{i+1} - a_i) \in I^n$, which implies that the sequence $\{a_n\}$ is Cauchy in the I-adic metric. Define the mapping $\Phi : \varprojlim A/I^n \to \widehat{A}_I$ by

$$(a_1 + I, a_2 + I^2, \ldots) \mapsto [a_n]$$

where as before $[a_n]$ is the equivalence class of $\{a_n\}$.
One then has to show that Φ is well defined, bijective and preserves ring operations. □

Example: 1. Let R be a commutative ring. Then $R[[x]] \cong \varprojlim_{n\in\mathbb{N}} R[x]/(x^n)$.

2. Let $l \geq 2$ be an integer. Then $\widehat{\mathbb{Z}}_l \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/l^n\mathbb{Z}$.

Proof of Theorem 27.1(c). Let $l = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. By Theorem 27.2 $\widehat{\mathbb{Z}}_l \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/l^n\mathbb{Z}$. Since $l^n = p_1^{\alpha_1 n} \dots p_k^{\alpha_k n}$, by the Chinese Remainder Theorem

$$\mathbb{Z}/l^n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1 n}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{\alpha_k n}\mathbb{Z}.$$

Hence

$$\widehat{\mathbb{Z}}_l \cong \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p_1^{\alpha_1 n}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{\alpha_k n}\mathbb{Z}) \cong$$

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p_1^{\alpha_1 n}\mathbb{Z} \times \ldots \times \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p_k^{\alpha_k n}\mathbb{Z} \cong \widehat{\mathbb{Z}}_{p_1^{\alpha_1}} \times \ldots \times \widehat{\mathbb{Z}}_{p_k^{\alpha_k}} \cong \widehat{\mathbb{Z}}_{p_1} \times \ldots \times \widehat{\mathbb{Z}}_{p_k}$$

where the last isomorphism holds by Theorem 27.1(b) and the second isomorphism is left as an exercise. □

Finally, we define the field of p-adic numbers. If p is prime, then as we proved $\widehat{\mathbb{Z}}_p$ is a domain, and we can consider its field of fractions $\mathbb{Q}_p$, called the field of p-adic numbers.

The analogue of Claim 26.1(2) for p-adic numbers asserts that any element of $\mathbb{Q}_p$ can be uniquely written as $\sum_{n=-N}^{\infty} a_n p^n$ where $0 \le a_n \le p-1$ and $N \in \mathbb{Z}$.

Remark: In the literature p-adic integers are most commonly denoted just by $\mathbb{Z}_p$. We used the more complex notation $\widehat{\mathbb{Z}}_p$ to avoid confusion with the use of $\mathbb{Z}_p$ for the finite field $\mathbb{Z}/p\mathbb{Z}$ (or cyclic group of order p).