MATH 6370, LECTURE 10
p-ADIC INTEGERS - THE BEST INTRODUCTION EVER
APRIL 08

GORDAN SAVIN

The ring of p-adic integers can be defined at once as the limit $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ of the inverse system of ring homomorphisms

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \dots .$$

Thus an element in $\mathbb{Z}_p$ is a sequence $x = (x_1, x_2, \dots)$ where x_{n-1} is the image of x_n under the natural projection map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$. The addition and multiplication operations are

$$x + y = (x_1 + y_1, x_2 + y_2, \dots) \text{ and } xy = (x_1y_1, x_2y_2, \dots)$$

where $x = (x_1, x_2, \dots)$ and $y = (y_1, y_2, \dots)$. The identity element is $1 = (1, 1, \dots)$, more generally we have a natural embedding $i : \mathbb{Z} \to \mathbb{Z}_p$ given by $i(x) = (x, x, \dots)$. An element $x = (x_1, x_2, \dots)$ is invertible if and only if ond only if all x_n are invertible. Since

$$(\mathbb{Z}/p^n\mathbb{Z})^\times = (\mathbb{Z}/p^n\mathbb{Z}) \setminus (p\mathbb{Z}/p^n\mathbb{Z}),$$

it follows that

$$\mathbb{Z}_p^\times = \lim_{\leftarrow}(\mathbb{Z}/p^n\mathbb{Z}_p)^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

If for a ring R, there exists an ideal $M \subset R$ such that $R^\times = R \setminus M$, then M is a unique maximal ideal in R. (Check it). Such ring is called a local ring. Thus $\mathbb{Z}_p$ is a local ring with $p\mathbb{Z}_p$ its maximal ideal. Observe that $i(x)$ is invertible for all integers x prime to p.

Exercise: Prove that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

There is another way to define $\mathbb{Z}_p$, as a completion of $\mathbb{Z}$ under p-adic metric. More precisely, every integer $x \neq 0$ can be written uniquely written $x = yp^n$ where y is prime to p. Define p-adic absolute value

$$|x| = \frac{1}{p^n}.$$

We also put $|0| = 0$. It is clear that $|xy| = |x| \cdot |y|$ for any $x, y \in \mathbb{Z}$. Moreover, the norm satisfies an inequality stronger than the triangular inequality

$$|x + y| \leq \max(|x|, |y|).$$

The norm defines a distance d on $\mathbb{Z}$ by $d(x, y) = |x - y|$. It satisfies

$$d(x, z) \leq \max(d(x, y), d(y, z))$$

so it is called ultra-metric. We define $\mathbb{Z}_p$ to be the completion of $\mathbb{Z}$ with respect to d. (This is abuse of notation, but we shall prove that two definitions are equivalent.) Thus $\mathbb{Z}_p$ is the set of equivalence classes of Cauchy sequences in $\mathbb{Z}$. Recall that (x_n) is a Cauchy sequence if for every $\epsilon > 0$ there exists and integer N such that

$$d(x_n, x_m) < \epsilon$$

for all $n, m > N$. If (x_n) and (y_n) are two Cauchy sequences, then the sequence of distances $d(x_n, y_n)$ is a Cauchy sequence of real numbers, hence it has a limit. If the limit is 0, then the two sequences are equivalent i.e. represent the same point in the completion. The set $\mathbb{Z}_p$ is naturally a ring, by adding and multiplying Cauchy sequences term by term.

Exercise: Let $p = 2$. Prove that the series $\sum_{n=1}^{\infty} 2^{n-1}$ is convergent (find its limit).

We shall prove that the two definitions produce isomorphic rings.

Lemma 0.1. *A sequence (x_n) in $\mathbb{Z}$ is Cauchy if and only if for every $\epsilon > 0$ there exists N such that*

$$d(x_n, x_{n+1}) < \epsilon$$

for all $n > N$.

Proof. This is saying that Cauchy sequences are characterized by a weaker condition. But this weaker condition suffices since the distance is ultra-metric, if $m > n$ then

$$d(x_n, x_m) \leq \max(d(x_n, x_{n+1}), \ldots, d(x_{m-1}, x_m)).$$

□

Now we can prove that the two definitions are equivalent. Let $x = (x_1, x_2, \ldots) \in \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. Let $z_n \in \mathbb{Z}$ such that $z_n \mapsto x_n$ under the natural projection $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Since $x_{n+1} \mapsto x_n$ under the projection $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, it follows that $z_{n+1} \equiv z_n \pmod{p^n}$. In other words, $d(z_n, z_{n+1}) \leq 1/p^n$, for all n, hence (z_n) is a Cauchy sequence in $\mathbb{Z}$ by the above lemma.

Conversely, let (y_n) be a Cauchy sequence in $\mathbb{Z}$. Recall that any subsequence of (y_n) is equivalent, that is, it represents the same point in the completion. Pick a subsequence (z_n) such that $d(z_n, z_{n+1}) \leq 1/p^n$ for all n. (Check that this can be done.) In other words $z_{n+1} \equiv z_n \pmod{p^n}$. Let x_n be the image of x_n under the projection $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Then $(x_1, x_2, \ldots)$ is an element in $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. It is easy to check that these maps are inverses of each other, hence the two definitions of p-adic numbers coincide.

Thie notion of p-adic completions generalizes to all number fields. Let A be the ring of integers in a number field, and fix $P \subset A$ a maximal ideal. Let q be the order of the finite field A/P. The P-adic norm on A is defined as follows: if $x \in A$ is non-zero, factor the principal ideal $(x) = P^n \cdot \ldots$ into a product of primes, where only the exponent of P is of interest. Put $|x| = q^{-n}$. The completion A_P of A is isomorphic to the inverse limit of quotients A/P^n. Let's look at the example $A = \mathbb{Z}[i]$ and $P = (1+i)$. Then $A_P = \mathbb{Z}_2[i]$ by the following:

Exercise: Let $|\cdot|$ be the 2-adic norm on $\mathbb{Z}$. Let $||\cdot||$ be the norm on $\mathbb{Z}[i]$ defined by

$$||x + iy|| = \max(|x|, |y|).$$

Prove that $||\cdot||$ is equivalent to the $(1+i)$-adic norm on $\mathbb{Z}[i]$. Hint: $(1+i)^2 = (2)$.