P-adic integers

Let $p \in \mathbb{P}$ be fixed.

For $n \in \mathbb{N}$ let $v_p(n) = \tau$ if $p^\tau \| n$ i.e. $n = p^\tau n_0$, $p \nmid n_0$

p-adic valuation

and define $|n|_p = p^{-\tau}$ if $p^\tau \| n$ so $|n|_p = p^{-v_p(n)}$.

Prop 10.1 (a) $|n+m|_p \leq \max(|n|_p, |m|_p) \leq |n|_p + |m|_p$.

(b) $|n \cdot m|_p = |n|_p \cdot |m|_p$

Pf (a) Suppose $p^s \| n$, $p^t \| m$ $(s, t \geq 0)$ then $p^{\min(s,t)} \mid n+m$

$$\Rightarrow v_p(n+m) \geq \min(s,t) \Rightarrow |n+m|_p \leq p^{-\min(s,t)} =$$

$$= \max(p^{-s}, p^{-t}) = \max(|n|_p, |m|_p).$$

(b) Clearly $p^{s+t} \| nm \Rightarrow$ (b) □

Note • Thus $d(n,m) := |n-m|_p$ is a metric.

We'll write $v_p(0) = \infty \Leftrightarrow |0|_p = 0$.

• This metric defines a strange topology on $\mathbb{Z}$.

We have $|n|_p = 1 \Leftrightarrow p \nmid n$

and $|n|_p = \rho = p^{-r}$ if $p^r \| n$

Consider the ball $B(n, \rho) = \{m ; |n-m| < \rho\}$;

these open balls defines the base of a topology for

the metric $d(x,y) = |x-y|_p$.

- $m \in B_{n,\rho}$, with $\rho = p^{-r} \iff |n-m|_p < p^{-r} \iff |n-m|_p \le p^{-r-1}$

  so $B_{n,p^{-r}} = \bar{B}_{n,p^{-r-1}} \Rightarrow B_{n,p^{-r}}$ both open and closed.

In fact $m \in \bar{B}_{n,p^{-r}} \iff p^r \mid n-m \iff n \equiv m \pmod{p^{r+1}}$

Thus $\forall r$: $\mathbb{Z} = \overset{p^{r-1}}{\underset{n=0}{\overset{*}{\bigcup}}} \bar{B}(n, p^{-r})$ covered by finitely many balls of radius p^{-r}.

<u>P-adic integers $\mathbb{Z}_p$</u> Consider $(\mathbb{Z}, d_p)$ metric space.

We construct the completion of $(\mathbb{Z}, d_p)$ via Cauchy-seq's (similarly as $\mathbb{R}$ is defined as C-seq's of rational numbers by "filling the holes" in $\mathbb{Q}$).

Let $x = (x_j)_{j=1}^{\infty}$ be a C-seq on $\mathbb{Z}$ with respect to d_p.

Let $k \in \mathbb{N}$, then $\exists\, J = J_k$ s.t. $|x_i - x_{j'}|_p \le p^{-k}$ $\forall i,j' \ge J_k$

$\iff x_i \equiv x_{j'} \pmod{p^k}$

Thus $\exists \lim_{j\to\infty} x_j \pmod{p^k} = s_k$, for some $0 \le s_k < p^k$.

moreover $s_{k+1} \pmod{p^k} = s_k$ for all $k \in \mathbb{N}$.

(as $\exists\, m \ge m_k$ s.t. $\left.\begin{aligned} x_m \pmod{p^{k+1}} &= s_{k+1} \\ x_m \pmod{p^k} &= s_k \end{aligned}\right\} \Rightarrow s_{k+1} \equiv s_k \pmod{p^k}$

We may write $\sigma = (s_k)_{j=1}^{\infty}$ then $|x_j - s_j|_p \to 0$ as $j \to \infty$

We say that $x = (x_j)_{j=1}^{\infty}$ and $y = (y_j)_{j=1}^{\infty}$ are equivalent $x \sim y$ if $|x_j - y_j|_p \to 0$ as $j \to \infty$.

Define $\mathbb{Z}_p = \{ [x], x = (x_j)_{j=1}^{\infty}$ being a Cauchy-sequence $\}$.

Lemma (Completion of metric spaces)

(i) $(\mathbb{Z}_p, d_p)$ complete where $d_p(x, y) = \lim_{j \to \infty} d_p(x_j, y_j)$

(ii) $\mathbb{Z} \subseteq \mathbb{Z}_p$ dense

(iii) Every element of $\mathbb{Z}_p$ has a representative

$x = (x_j)_{j=1}^{\infty}$ s.t. $x_{j+1} \equiv x_j \pmod{p^j}$ for all $j \geq 0$.

Pf (i) – holds for general metric spaces

(ii) also, but easy to see.

Indeed, if $x \in \mathbb{Z}$ then let $x_j := x \pmod{p^j}$ $(0 \leq x_j < p^j)$

this gives an embedding $\iota : \mathbb{Z} \hookrightarrow \mathbb{Z}_p$

but if $x = (x_j)_{j=1}^{\infty}$ then $x = \lim_{j \to \infty} \iota(x_j)$

However $|x_k - x_j|_p \leq p^{-j}$ for all $k \geq k(j)$

$\Rightarrow d_p(x, x_j) \leq p^{-j} \Rightarrow$ ↙

(iii) We have shown this already.

- $\mathbb{Z}_p$ as an Abelian group (ring) $x = (x_j)$, $y = (y_i)$
  then clearly with $x + y := (x_j + y_j)$, $x \cdot y = (x_j \cdot y_j)$
- one has: $x + y = y + x$, $x + (-x) = 0$, $0 + x = x$
- $(\mathbb{Z}_p, +)$ is a compact Abelian group. this follows from

(i) $\mathbb{Z} \subseteq \mathbb{Z}_p$ dense, $\mathbb{Z}_p$ complete

(ii) $\mathbb{Z}$ is totally bounded, i.e. $\mathbb{Z} = \bigcup_{n=0}^{p^r-1} B(n, p^{-r})$, $\forall r \geq 0$

Pf Let $(x_m)_{m \geq 1} \subseteq \mathbb{Z}_p$ sequence. $\exists n_1$ s.t. $B(n_1, p^{-1})$ contain a subseq.

$\exists n_2$ s.t. $B(n_2, p^{-2}) \subseteq B(n_1, p^{-1})$ contains a subseq

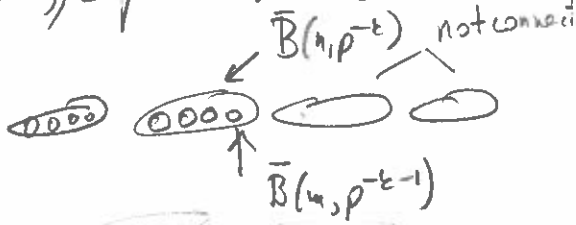
$\exists n_k$ s.t. $B(n_k, p^{-k}) \subseteq$ —

$\Rightarrow$ take the diagonal subsequence; it is a Cauchy hence a convergent subseq.

- (Haar) measure on $\mathbb{Z}_p$. Define the algebras

$\mathcal{B}_k$ generated by $\bar{B}(n, p^{-k})$ $(0 \leq n < p^k)$; and

$\mu_k : \mathcal{B}_k \mapsto [0,1]$ s.t. $\mu_k(\bar{B}(n, p^{-k})) = p^{-k}$ $\forall n$,



Note, that $\mathcal{B}_k \subseteq \mathcal{B}_{k+1}$

and $\mu_{k+1} \mid \mathcal{B}_k = \mu_k$

There exists a weak limit $\mu =: \lim_{i \to \infty} \mu_{k_i}$, on $\mathcal{B} = \bigvee_{1}^{\infty} \mathcal{B}_k$

Also, $\mu_k(m+\bar{B}(n,p^{-k})) = \mu_k(\bar{B}(n+m,p^{-k})) = p^{-k}$ $\forall m,n$

$\Rightarrow$ $\mu_k(m+B) = \mu_k(B)$ $\forall B \in \mathcal{B}_k$ $\forall k$

$\Rightarrow$ $\mu(m+B) = \mu(B)$ $\forall B \in \mathcal{B}$.

- Waring problem over $\mathbb{Z}_p$

Let $N \in \mathbb{N}$, $x_1 = (x_{1j})_{j=1}^{\infty}, \dots, x_s = (x_{sj})_{j=1}^{\infty} \in \mathbb{Z}_p$ (in canonical form).

Consider the equation: $x_1^k + \dots + x_s^k = N$ in $\mathbb{Z}_p$. (1)

Since $d_p(x_i, x_{ij}) = \lim_{m\to\infty} |x_{im} - x_{ij}|_p \le p^{-j}$

(as $|x_{im} - x_{ij}| \le p^{-j}$ $\forall m \ge j$)

One has

$$d_p(x_i^k - x_{ij}^k) = |(x_i - x_{ij})(x_i^{k-1} + x_i^{k-2}x_{ij} + \dots + x_{ij}^{k-1})|_p$$

$$\le |x_i - x_{ij}|_p \left(\max_\ell |x_i^{k-\ell} x_{ij}^{\ell}|_p\right) \le |x_i - x_{ij}|_p \le p^{-j}$$

It follows $|x_{1j}^k + \dots + x_{sj}^k - N|_p \le p^{-j}$

$$\Rightarrow \quad x_{1j}^k + \dots + x_{sj}^k \equiv N \pmod{p^j} \text{ for all } j \ge 1 \quad (2)$$

Thus a solution to (1) in $\mathbb{Z}_p$ is equivalent to a simultaneous solution of the congruences

$$\left.\begin{aligned} x_{ij}^k + \cdots + x_{sj}^k &\equiv N \pmod{p^j} \\ \text{with} \quad x_{ij+1} &\equiv x_{ij} \pmod{p^j} \end{aligned}\right\} \text{ for all } j \geq 1.$$

Note that we have constructed exactly these type of solutions.