Algebraic NT, L4 Building up $\mathbb{C}_p$

$\mathbb{C}_p$ is the p-adic variant of $\mathbb{C}$, the p-adic complex numbers. But first we have to explain what symbols like $\mathbb{Q}_p$ or $\mathbb{Z}_p$ (not $\mathbb{Z}$ mod p!) mean.

We begin with metric spaces. Recall that

(X,d) is a m. sp. if X is a set and $d: X\times X \to [0,+\infty)$ the metric satisfies:

(1) $d(x,y)=0 \iff x=y$
(2) $d(x,y)=d(y,x)$
(3) $d(x,y)\le d(x,z)+d(z,y)$ (Δ-ineq.)

Usually $X=F$, a field, and $d(\cdot,\cdot)$ comes from a norm $\|\cdot\|$ on F: $\|\cdot\|: F\to[0,+\infty)$ satisfies:

(1) $\|x\|=0 \iff x=0_F$
(2) $\|xy\|=\|x\|\cdot\|y\|$
(3) $\|x+y\|\le\|x\|+\|y\|$

$\rightsquigarrow$ $d(x,y):=\|x-y\|$ is a metric on F (easy to see)

Example Usual $|\cdot|$ on the field $\mathbb{Q}$, $d(x,y)=|x-y|$ is the usual Euclidean metric on rational numbers.

Example F any field, $\|x\|=\begin{cases}0 & \dots x=0_F\\ 1 & \dots x\neq 0_F.\end{cases}$ This

is the trivial norm.

Example $F=\mathbb{Q}$, p a prime number, for $\alpha\in\mathbb{Q}^\times$ we define $\mathrm{ord}_p(\alpha) :=$ the unique $n\in\mathbb{Z}$ s.t. $\alpha = p^n \frac{a}{b}$, $a,b\in\mathbb{Z}$ both coprime to p. For $\alpha=0$ we set $\mathrm{ord}_p(0) := +\infty$.

We define the p-adic norm on $\mathbb{Q}$ by ($\alpha\in\mathbb{Q}$)

$$\|\alpha\|_p := p^{-\mathrm{ord}_p(\alpha)} = \left(\frac{1}{p}\right)^{\mathrm{ord}_p(\alpha)}.$$ So $\|0\|_p := 0$. One can show that $\|\cdot\|_p$ is a norm on the field $\mathbb{Q}$. Unlike $|\cdot|$, $\|\cdot\|_p$ is a non-Archimedean norm. These are norms satisfying the strong Δ-ineq., namely

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

the corresponding metric $d(x,y)=\|x-y\|$ then satisfies the:

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

- non-Arch. metric or
- ultrametric

$\rightsquigarrow$ $d(x,z)\neq d(z,y) \Rightarrow =$ in

$\rightsquigarrow$ In an ultrametric space all Δs are equilateral

$\rightsquigarrow$ —— " —— every point in a ball (no matter whether open or closed) is its center.

Ball: $\{x\in X \mid d(x,c)<r\}$, $c\in X$, $r>0$.

A sequence $(a_n) \subset X$ in a metr. space (X,d) is Cauchy:

$(\forall \varepsilon > 0 \; \exists n_0 : n, m \geq n_0 \Rightarrow d(a_m, a_n) < \varepsilon$.

Two metrics are equivalent: they have the same C. (on the same set X) sequences. Two norms on a field F are equivalent: have equivalent corresponding metrics.

One can show that norms on $\mathbb{Q}$ eq. to $|\cdot|$ (absolute value) are exactly of the form $|\cdot|^\alpha$ for real α, $0 < \alpha \leq 1$. Similarly, one can show that norms on $\mathbb{Q}$ eq to $\|\cdot\|_p$ (p-adic norm) are exactly of the form $s^{\mathrm{ord}_p(\cdot)}$ for real s, $0 < s < 1$.

We have the next thm.

(Theorem 4 (Ostrowski) Every norm on $\mathbb{Q}$ is either the trivial norm, or is eq. to $|\cdot|$, or is eq. to $\|\cdot\|_p$ for some prime p. Proof. See the book [Kob], pp. 3-5] or my lecture notes from MA III.

(To get to Ω, let's recall how we get the fields $\mathbb{R}$ and $\mathbb{C}$. $\mathbb{R}$ is the metric closure of $\mathbb{Q}$, w.r.t. $|\cdot|$.

this means that $(\mathbb{Q}, |\cdot|) \subset (\mathbb{R}, |\cdot|)$ (as normed fields), $\mathbb{Q}$ is dense in $\mathbb{R}$ and $(\mathbb{R}, |\cdot|)$ is complete, every C. sequence $(a_n) \subset \mathbb{R}$ has a limit $a \in \mathbb{R}$ $(\forall \varepsilon > 0 \; \exists n_0 : n \geq n_0 \Rightarrow |a - a_n| < \varepsilon)$.

$\mathbb{R} \subset \mathbb{C}$ (as fields) and $\mathbb{C} = \overline{\mathbb{R}}$ - every $z \in \mathbb{C}$ is algebraic over $\mathbb{R}$ and $\mathbb{C}$ is alg. closed $(\forall p(z) \in \mathbb{C}[z] \; \exists z_0 \in \mathbb{C}$ s.t. $p(z_0) = 0)$. In fact, $[\mathbb{C} : \mathbb{R}] = 2$ because $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\}$ and $i^2 = -1$. Thus $\mathbb{C}$ arises from $\mathbb{R}$ be adding to $\mathbb{R}$ a root of -1. The field $\mathbb{C}$ also remains complete (as it is only a finite extension of $\mathbb{R}$).

We parallel this construction for the p-adic norm $\|\cdot\|_p$ (and field $\mathbb{Q}$). First we get the metric closure $(\mathbb{Q}_p, \|\cdot\|_p)$ of $(\mathbb{Q}, \|\cdot\|_p)$. The field $\mathbb{Q}_p$ is called the field of p-adic numbers.

Then we take the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Unfortunately, now $[\overline{\mathbb{Q}}_p : \mathbb{Q}_p] = \infty$ and, as a consequence, $\overline{\mathbb{Q}}_p$ is not complete. So we have to take another metric closure $(\overline{\mathbb{Q}}_p, \|\cdot\|_p)$

and get the field $(\mathbb{L}\mathbb{L}, \|\cdot\|_p)$. Fortunately, $\mathbb{L}\mathbb{L}$ remains alg. closed. Thus $\mathbb{L}\mathbb{L}$ may serve as p-adic analog of $\mathbb{C}$.

We look more closely on $\mathbb{Q}_p$. Let $S = \{(a_n) \subset \mathbb{Q} \mid (a_n) \text{ is C. w.r.t. } \|\cdot\|_p\}$. For $(a_n), (b_n) \in S$ we set $(a_n) \sim (b_n) \Leftrightarrow \forall \varepsilon > 0 \, \exists n_0 : n, k \geq n_0 \Rightarrow \|a_n - b_k\| < \varepsilon$. We define $\mathbb{Q}_p$ to be the set of equiv. classes w.r.t. $\sim$:

$$\boxed{\mathbb{Q}_p := S/\sim}$$

the field operations on $\mathbb{Q}_p$ and the (extended) norm are defined by:

$$[(a_n)]_\sim + [(b_n)]_\sim := [(a_n + b_n)]_\sim$$

$$[(a_n)]_\sim \cdot [(b_n)]_\sim := [(a_n b_n)]_\sim$$

$$\|[(a_n)]_\sim\|_p := \lim_{n \to \infty} \|a_n\|_p \in \{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

It is not hard but a little tedious to prove that: the above definitions := are all correct, independent of the concrete representatives of $[\cdot]$; we get a normed field $(\mathbb{Q}_p, \|\cdot\|_p)$ that extends $(\mathbb{Q}, |\cdot|_p)$ (in the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $a \mapsto [(a, a, a, \ldots)]_\sim$); $\mathbb{Q}$ is dense in

$\mathbb{Q}_p$; and $\mathbb{Q}_p$ is complete, i.e. every C. sequence $(a_n) \subset \mathbb{Q}_p$ has a limit.

More practical approach to $\mathbb{Q}_p$ (than via definition) is the next representation thm.

Theorem 5 Every eq.-class $a = [(a_n)]_\sim$ in $\mathbb{Q}_p$ has a unique representative $(c_n) \subset \mathbb{N}_0$ s.t.

(1) $\forall n \in \mathbb{N}: 0 \leq c_n < p^n$.

(2) $\forall n \in \mathbb{N}: c_n \equiv c_{n+1} \pmod{p^n}$.

Thank you!