Lecture 22 The p-adic field $\mathbb{Q}_p$

Let p be a prime number. The ring of p-adic integers is

$$\mathbb{Z}_p := \varprojlim_i \mathbb{Z}/p^i\mathbb{Z} = \left\{ (\dots, x_2, x_1) \in \prod_{i \geqslant 1} \;\middle|\; \forall\, i \geqslant j : \pi_{ij}(x_i) = x_j \right\},$$

where for each $i \geqslant j$ the inclusion

$$p^i\mathbb{Z} \subseteq p^j\mathbb{Z}$$

yields the surjective ring homomorphism

$$\pi_{ij} : \mathbb{Z}/p^i\mathbb{Z} \longrightarrow \mathbb{Z}/p^j\mathbb{Z}.$$

Prop'n If $(X_\alpha, \pi_{\alpha\beta})$ is an inverse system of Hausdorff spaces, then its inverse limit

$$X := \varprojlim X_\alpha$$

is Hausdorff. Moreover, $X \subseteq \prod_\alpha X_\alpha$ is a closed subspace.

Proof – following Bourbaki.[1]

As subspace of a Hausdorff space, X is Hausdorff. Moreover, for each $\alpha \leqslant \beta$ we have a closed set

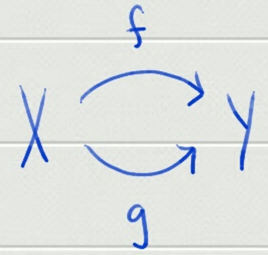
$$F_{\alpha\beta} := \left\{ x \in \prod_\alpha X_\alpha \;\middle|\; \pi_\alpha(x) = (\pi_{\alpha\beta} \circ \pi_\beta)(x) \right\}.$$

---

1. See Corollary 2 (p. 78), no. 2, § 8, Ch. I, Bourbaki, N., *Elements of Mathematics*, 18, Springer-Verlag, 2013.

Indeed, this follows from the following.

Lemma (Bourbaki[2]) For continuous functions



where Y is assumed Hausdorff, the set

$$C := \{ x \in X \mid f(x) = g(x) \}$$

is closed.

---

2. See Proposition 2 (p. 76), no. 1, § 8, Ch. I, *idem*. It yields the *Principle of extension of identities*: if we further assume that C is dense, then $f = g$.

But

$$\varprojlim X_\alpha = \bigcap_{\alpha \leq \beta} F_{\alpha\beta},$$

hence the limit is closed $\square$

For each $i \in \mathbb{Z}_{\geq 1}$ give $\mathbb{Z}/p^i\mathbb{Z}$ the discrete topology. From the above we see that $\mathbb{Z}_p$ is thus a compact topological ring. Moreover, the natural map

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p$$

$$x \longmapsto (\ldots, \pi_2(x), \pi_1(x))$$

is an injective ring homomorphism onto a dense subset of $\mathbb{Z}_p$. Indeed, $\forall\, x_i \in \mathbb{Z}/p^i\mathbb{Z}$

$$x_i = \overline{a_0 + a_1 p + \dots + a_{i-1} p^{i-1}}$$

with $a_0, \dots, a_{i-1} \in \{0, \dots, p-1\}$ uniquely determined.

Lemma An element $x \in \mathbb{Z}/p^i\mathbb{Z}$ is invertible if and only if $p \nmid x$.

Proof

($\Leftarrow$): We have an exact sequence

$$0 \longrightarrow p(\mathbb{Z}/p^i\mathbb{Z}) \longrightarrow \mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\pi_{i1}} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

$$\overline{a_0 + a_1 p + \dots + a_{i-1} p^{i-1}} \longmapsto \overline{a_0}$$

As $x \notin p(\mathbb{Z}/p^i\mathbb{Z})$, then $\pi_{i1}(x) \neq 0$, so $\pi_{i1}(x) \in \mathbb{F}_p^{\times}$.

This means that $\exists\ y, z \in \mathbb{Z}/p^i\mathbb{Z}$ s.t.

$$xy = 1 - pz$$

But

$$(1 + pz + \cdots + p^{i-1}z^{i-1})(1 - pz) =$$

$$1 + pz + \cdots + p^{i-1}z^{i-1} - (pz + \cdots + p^i z^i) =$$

$$1 - p^i z^i = 1$$

Hence the element

$$y(1 + pz + \cdots + p^{i-1}z^{i-1})$$

is the inverse of x.

($\Rightarrow$): We may express each $x \in \mathbb{Z}/p^i\mathbb{Z}$ as

$$x = \overline{a_0 + a_1 p + \dots + a_{i-1} p^{i-1}} \qquad (a_k \in \{0, \dots, p-1\})$$

So $x \in (\mathbb{Z}/p^i\mathbb{Z})^\times$ implies that $x \notin p(\mathbb{Z}/p^i\mathbb{Z})$. $\square$

Corollary The ring $\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal

$$\mathfrak{m} = p\mathbb{Z}_p$$

and $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \mathfrak{m}$. So for every nonzero $x \in \mathbb{Z}_p$ we have

$$x = u\, p^{v(x)}$$

where $u \in \mathbb{Z}_p^\times$ and $v(x) \in \mathbb{Z}_{\geq 0}$ are uniquely determined by x.

Let $\mathbb{Q}_p$ be the field of fractions of $\mathbb{Z}_p$. In fact $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$ and we have an exact sequence

$$1 \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0$$

So $\mathbb{Q}^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$. In order to describe the structure of the multiplicative group $\mathbb{Z}_p^\times$ we'll show that we have a further exact sequence

$$1 \longrightarrow 1+m \longrightarrow \mathbb{Z}^\times \longrightarrow \mu_{p-1} \longrightarrow 1$$

$$x \longmapsto \omega(x) := \lim_{i \to \infty} x^{p^i}$$

The group homomorphism

$$\omega : \mathbb{Z}^\times \longrightarrow \mu_{p-1}$$

is known as the *Teichmüller character*. One may show that the sequence $\{x^{p^i}\}_{i=1}^{\infty}$ is a Cauchy sequence, so by the completeness of $\mathbb{Z}_p$ it must converge.

Moreover, for each $i \in \mathbb{Z}_{\geq 1}$

$$\left(x^{p^i}\right)^p = x^{p^{i+1}}$$

So $\omega(x)^p = \omega(x)$, and thus $\omega(x)^{p-1} = 1$, so the homomorphism ω is well-defined. Moreover, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p^\times & \xrightarrow{\omega} & \mu_{p-1} \\ \downarrow{\scriptstyle \pi_1} & \swarrow{\scriptstyle \pi_1 | \mu_{p-1}} & \\ \mathbb{F}_p^\times & & \end{array}$$

In particular, for each $x \in \mathbb{Z}$ we have the congruence

$$\omega(x) \equiv x \pmod{p}.$$

For example, if $p = 5$ then we explicitly have

$$\omega(1) = 1$$

$$\omega(2) = 2 + 1 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots$$

$$\omega(3) = 3 + 3\cdot 5^1 + 2\cdot 5^2 + 3\cdot 5^3 + 1\cdot 5^4 + \dots$$

$$\omega(4) = 4 + 4\cdot 5^1 + 4\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + \dots = -1$$

The sequence $\tau_i := \omega(i)$, $i \in \{0, \dots, p-1\}$ is known as the Teichmüller representatives and yield a more natural way to express the p-adic numbers, as opposed to the set $\{0, 1, \dots, p-1\}$.