Notes on Number Theory

Ken Lee

Summer 2020

Contents

These are notes based on Serre's "*A Course in Arithmetic*", with bits added here and there from various sources like Atiyah, nlab, etc.

1 p-adic Fields

In the following section, let $p \in \mathbb{Z}$, $0 < p$ be a prime.

1.1 $\mathbb{Z}_p$ and $\mathbb{Q}_p$

Definition – Projective System

Let $\mathbb{N}$ be the naturals viewed as a category with the usual ordering. Let $\mathcal{C}$ be a category. Then a *projective system in $\mathcal{C}$* is a contravariant functor from $\mathbb{N}$ to $\mathcal{C}$. For a projective system F, we will denote the image of the morphism $k \leq l$ with $\downarrow_k^l$.

Equivalently, a projective system in $\mathcal{C}$ is a collection of objects $(F_n)_{n\in\mathbb{N}}$ in $\mathcal{C}$ together with a collection of maps $(\downarrow_n^{n+1} : F_{n+1} \to F_n)_{n\in\mathbb{N}}$ such that for all $n \in \mathbb{N}$, $\downarrow_n^{n+1}\downarrow_{n+1}^{n+2}=\downarrow_n^{n+2}$.

Definition – Inverse Limit of a Projective System

Let $\mathcal{C}$ be a category and $F : \mathbb{N}^{op} \to \mathcal{C}$ be a projective system. Then an *inverse limit of F* is just a limit of F as an $\mathbb{N}^{op}$-diagram.

Definition – p-adic Integers

Define the following projective system of commutative rings, $\mathbb{Z}/p^\star\mathbb{Z}$ by :

1. $n \in \mathrm{Obj}\,(\mathbb{N}^{op}) \mapsto \mathbb{Z}/p^n\mathbb{Z}$

2. For $n \in \mathbb{N}^{op}$, $\downarrow_n^{n+1}$: $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the natural projection (from the universal property of $\mathbb{Z}/p^{n+1}\mathbb{Z}$).

Then the *p-adic integers* $\mathbb{Z}_p$ is defined as the inverse limit of $\mathbb{Z}/p^\star\mathbb{Z}$. For $n \in \mathbb{N}$, $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ will denote the projection that comes with the definition of $\mathbb{Z}_p$ as a limit.

We have an explicit construction of $\mathbb{Z}_p$ as the subset of $x \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ such that for all $n \in \mathbb{N}$, $\downarrow_n^{n+1} \varepsilon_{n+1}(x) = \varepsilon_n(x)$.

Remark – Meaning of p-adic integers. One should think of p-adic integers along the following analogy with complex analysis :

1. $\mathbb{Z}$ is the ring of holomorphic functions on a space, the space being the set of primes of $\mathbb{Z}$.
2. A prime p is a point.
3. Taking an integer f to $\mathbb{Z}/p\mathbb{Z}$ is evaluation of the function f at the point p.
4. Sending an integer f to $\mathbb{Z}/p^n\mathbb{Z}$ is the taylor expansion of f at p up to terms of order n. You can write f in $\mathbb{Z}/p^n\mathbb{Z}$ as a polynomial in $1, p, \ldots, p^{n-1}$ with coefficients in $\{0, \ldots, p-1\}$.
5. Elements of $\mathbb{Z}_p$ are precisely coherent collections of taylor expansions of higher and higher order, i.e. power series in p. This is formalized later.

Proposition – $\mathbb{Z}$ injects into $\mathbb{Z}_p$

The canonical ring morphism $\mathbb{Z} \to \mathbb{Z}_p$ has kernel $\bigcap_{n\in\mathbb{N}} p^n\mathbb{Z} = 0$.

Proof. Clear from the construction of $\mathbb{Z}_p$. □

Proof. We have a short exact sequence of projective systems in $\mathbb{Z}$-**Mod**,

$$0 \longrightarrow p^\star\mathbb{Z} \longrightarrow \underline{\mathbb{Z}} \longrightarrow \mathbb{Z}/p^\star\mathbb{Z} \longrightarrow 0$$

where the middle projective system is a constant at $\mathbb{Z}$. Since limits commute with limits, taking the inverse limit is left exact and we obtain :

$$0 \longrightarrow \varprojlim n \in \mathbb{N}p^n\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \varprojlim n \in \mathbb{N}\mathbb{Z}/p^n\mathbb{Z}$$

The inverse limit of $\mathbb{Z}/p^\star\mathbb{Z}$ in $\mathbb{Z}$-**Mod** is still $\mathbb{Z}_p$. (This follows elementarily, or from the fact that the forgetful functor from **CRing** to $\mathbb{Z}$-**Mod** is a right adjoint, and hence it preserves limits.) And the inverse limit of $p^\star\mathbb{Z}$ is the intersection. □

Proposition – Truncation

Let $n \in \mathbb{N}$. Then we have the following short exact sequence in $\mathbb{Z}$-**Mod** :

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

Proof. (*Exactness at left*) It suffices to show that multiplying by p is an injection, i.e. you can cancel by p. Let $x \in \mathbb{Z}_p$ such that $px = 0$. Then for $k \in \mathbb{N}$, $0 = \varepsilon_{k+1}(px) = p\varepsilon_{k+1}(x)$ implies the existence of a $x_{k+1} \in \mathbb{Z}$ such that $x_{k+1} = \varepsilon_{k+1}(x)$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ and $p^{k+1} \mid px_{k+1}$. Then $p^k \mid x_{k+1}$, so $\varepsilon_k(x) =\downarrow_k^{k+1} \varepsilon_{k+1}(x) =\downarrow_k^{k+1} x_{k+1} = 0$. Therefore $\varepsilon_k(x) = 0$ for all $k \in \mathbb{N}$, i.e. $x = 0$.

(*Exactness at right*) ε_n is surjective.

(*Exactness in middle*) Clearly, $p^n\mathbb{Z}_p \subseteq \ker \varepsilon_n$. Let $x \in \ker \varepsilon_n$. In the following, for $k \in \mathbb{N}$, let $\pi_k : \mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be the natural projection. For $k \in \mathbb{N}$, let x_k be the unique integer in $\{0, \dots, p^k - 1\}$ such that $\pi_k(x_k) = \varepsilon_k(x)$ in $\mathbb{Z}/p^k\mathbb{Z}$. Then $\varepsilon_n(x) = 0$ implies for all $k \in \mathbb{N}$,

$$\pi_n(x_{n+k}) =\downarrow_n^{n+k} \pi_{n+k}(x_{n+k}) =\downarrow_n^{n+k} \varepsilon_{n+k}(x) = \varepsilon_n(x) = 0$$

that is to say $p^n \mid x_{n+k}$. Since $0 \le x_{n+k} < p^{n+k}$, there exists a unique $0 \le y_k < p^k$ such that $x_{n+k} = p^n y_k$ in $\mathbb{Z}$. Let $y \in \prod_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ such that for all $k \in \mathbb{N}$, $\varepsilon_k(y) = \pi_k(y_k)$. Then for $k \in \mathbb{N}$, $\pi_{n+k}(x_{n+k+1}) =\downarrow_{n+k}^{n+k+1} \varepsilon_{n+k+1}(x) = \varepsilon_{n+k}(x) = \pi_{n+k}(x_{n+k})$ implies $p^{n+k} \mid x_{n+k+1} - x_{n+k} = p^n(y^{k+1} - y^k)$, and therefore $p^k \mid y^{k+1} - y^k$. Hence $y \in \mathbb{Z}_p$. Then for $k \in \mathbb{N}$,

$$\varepsilon_k(p^n y) = \pi_k(p^n y_k) =\downarrow_k^{n+k} \pi_{n+k}(p^n y_k) =\downarrow_k^{n+k} \pi_{n+k}(x_{n+k}) =\downarrow_k^{n+k} \varepsilon_{n+k}(x) = \varepsilon_k(x)$$

Therefore, $x = p^n y \in p^n\mathbb{Z}_p$. $\square$

Proof. (Generalized from nLab)

Consider the following short exact sequence of projective systems in $\mathbb{Z}$-$\mathbf{Mod}$:

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r, "p^n"] \arrow[d] & \mathbb{Z}/p^{n+2}\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r, "p^n"] \arrow[d] & \mathbb{Z}/p^{n+1}\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}
$$

Since the left system is surjective, by taking inverse limits we obtain the desired short exact sequence in $\mathbb{Z}$-$\mathbf{Mod}$:

$$
0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0
$$

$\square$

Remark – Meaning of Truncation. ε_n is precisely truncating a power series at terms of order n and higher. Then the theorem says the power series that are zero up to terms order n are precisely the ones consisting of terms of order n and higher.

> **Proposition – $\mathbb{Z}_p$ Local Ring**
> For $n \geq 1$, $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$. Hence $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$.

Proof. (Serre's)

Let $n \geq 1$. It suffices to show that $\mathbb{Z}/p^n\mathbb{Z} \setminus p\mathbb{Z}/p^n\mathbb{Z} \subseteq \mathbb{Z}/p^n\mathbb{Z}^\times$. Let $x \in \mathbb{Z}/p^n\mathbb{Z}$ be not divisible by p. Then there exists $y \in \mathbb{Z}/p^n\mathbb{Z}$ such that $\downarrow_1^n (xy) = 1$. Let $0 \leq x_n, y_n < p^n$ be representatives of x, y in $\mathbb{Z}$. Then there exists $z_n \in \mathbb{Z}$ such that $x_n y_n = 1 - pz_n$. Let $\pi_n : \mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the natural projection and $z := \pi_n(z_n)$. Then we have

$$xy(1+pz+\cdots+(pz)^{n-1})=\pi_n((1-pz_n)(1+pz+\cdots+(pz)^{n-1}))=\pi_n(1-(pz_n)^n)=1$$

Thus x is a unit.

To show $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$, it again suffices that $\mathbb{Z}_p \setminus p\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$. Let $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Then for all $n \geq 1$, $0 \neq \varepsilon_1(x) = \downarrow_1^n \varepsilon_n(x)$. Since $\downarrow_1^n$: $(\mathbb{Z}/p^n\mathbb{Z})/(p\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ as rings, $\varepsilon_n(x) \in \mathbb{Z}/p^n\mathbb{Z}^\times$ by the above. Let $y_n = \varepsilon_n(x)^{-1}$. Then uniqueness of inverses implies $\downarrow_n^{n+1} y_{n+1} = y_n$, i.e. there exists a unique $y \in \mathbb{Z}_p$ such that for all n, $\varepsilon_n(y) = y_n$. Then $xy = 1$, i.e. $x \in \mathbb{Z}_p^\times$. □

Proof. (via geometric series)

We show $\mathbb{Z}_p$ is local directly. Since $p\mathbb{Z}_p = \ker \varepsilon_1$ which is a maximal ideal in $\mathbb{Z}_p$, it suffices that $p\mathbb{Z}_p$ is the Jacobson radical of $\mathbb{Z}_p$, equivalently $1 - p\mathbb{Z}_p \subseteq \mathbb{Z}_p^\times$.

Let $x \in p\mathbb{Z}_p$. All we need to do is justify $1/(1-x) = \sum_{k=0}^\infty x^k$ is an element in $\mathbb{Z}_p$. For $k \in \mathbb{N}$, define $y_k := \sum_{0 \leq l < k} \varepsilon_k(x^l) \in \mathbb{Z}/p^k\mathbb{Z}$ and let y be the unique element in $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ such that for all $k \in \mathbb{N}$, $\varepsilon_k(y) = y_k$. Then $x \in p\mathbb{Z}_p$ implies $x^k \in p^k\mathbb{Z}_p = \ker \varepsilon_k$, which shows that $y \in \mathbb{Z}_p$ and is the desired inverse of $1 - x$. □

Remark – Why $\mathbb{Z}_p$ is a Local Ring. This is the analogue of the fact that a power series is invertible if and only if its constant coefficient is invertible.

> **Definition – Naturals with Infinity**
> Let $\mathbb{N}^\infty := \mathbb{N} \sqcup \{\infty\}$. Define $\leq$ on $\mathbb{N}^\infty$ as follows :
>
> - For all $n, m \in \mathbb{N}^\infty \setminus \{\infty\}$, $n \leq m$ is as usual.
> - For all $n \in \mathbb{N}^\infty$, $n \leq \infty$.
>
> Define $+$ on $\mathbb{N}$ as follows :
>
> - For $n, m \in \mathbb{N}^\infty \setminus \{\infty\}$, $n + m$ is as usual.
> - For $n \in \mathbb{N}^\infty$, $n + \infty = \infty$.

> **Definition – p-adic Valuation, Norm**
> The *p-adic valuation* is defined as the following :
>
> $$v_p : \mathbb{Z}_p \longrightarrow \mathbb{N}^\infty, x \mapsto \sup\{n \in \mathbb{N}^\infty \mid \varepsilon_n(x) = 0\}$$
>
> From this, we define the *p-adic norm*,
>
> $$|\star|_p : \mathbb{Z}_p \longrightarrow [0,\infty) \subseteq \mathbb{R}, x \mapsto \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0 \end{cases}$$

Remark – Meaning of p-adic Norm. Continuing the analogy, $|\star|_p$ formalizes the idea that higher order terms are smaller and in the limit, zero.

Proposition – Unique Decomposition in $\mathbb{Z}_p$

Let $x \in \mathbb{Z}_p$, $x \neq 0$. Then

1. $v_p(x) \neq \infty$.
2. Since by definition, $\varepsilon_{v_p(x)}(x) = 0$ and multiplying by $p^{v_p(x)}$ is injective, there exists a unique $u(x) \in \mathbb{Z}_p$ such that $x = p^{v_p(x)}u(x)$. Then $u(x) \in \mathbb{Z}_p^\times$
3. For all $n \in \mathbb{N}$ and $u \in \mathbb{Z}_p^\times$, $x = p^n u$ implies $n = v_p(x)$ and $u = u(x)$

Proof.

(1) For $n \in \mathbb{N}$, $\varepsilon_n(x) = 0$ implies for all $k \leq n$, $\varepsilon_k(x) = 0$. Since $x \neq 0$, this implies the set of n such that $\varepsilon_n(x) = 0$ is bounded above by a natural $N \in \mathbb{N}$. Hence $v_p(x) \leq N < \infty$.

(2) Since $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$, it suffices to show that $u(x) \notin p\mathbb{Z}_p = \ker \varepsilon_1$. Well, if $u(x) \in p\mathbb{Z}_p$, then $x \in p^{v_p(x)} + 1\mathbb{Z}_p$, which implies $\varepsilon_{v_p(x)+1}(x) = 0$, contradicting the maximality of $v_p(x)$.

(3) Let $n \in \mathbb{N}$, $u \in \mathbb{Z}_p^\times$ such that $x = p^n u$. Already, $x \in p^n\mathbb{Z}_p$ implies $n \leq v_p(x)$ by definition of $v_p(x)$. Then $u \in p^{v_p(x)-n}\mathbb{Z}_p$ and $u \in \mathbb{Z}_p^\times$ implies $v_p(x) = n$. Then $u = u(x)$ since multiplying by $p^{v_p(x)}$ is injective. □

Proposition – $(\mathbb{Z}_p, |\star|_p)$ Normed Ring

The following are true :

1. (Positive Definite) For all $x \in \mathbb{Z}_p$, $|x|_p = 0$ if and only if $x = 0$.
2. (Ultrametric Property) For all $x, y \in \mathbb{Z}_p$, $|x+y|_p \leq \max(|x|_p, |y|_p)$.
3. (Multiplcative) For $x, y \in \mathbb{Z}_p$, $|xy|_p = |x|_p |y|_p$.
4. (Normalized) $|1|_p = 1$

Hence $\mathbb{Z}_p$ is a topological ring with the topology from $|\star|_p$.

Proof.

(1) Clear.

(2) It suffices to show $\min(v_p(x), v_p(y)) \leq v_p(x+y)$. Let $n = \min(v_p(x), v_p(y))$. Then $\varepsilon_n(x+y) = \varepsilon_n(x) + \varepsilon_n(y) = 0$. So $n \leq v_p(x+y)$ by its maximality.

(3) It suffices to show $v_p(xy) = v_p(x) + v_p(y)$. This follows from the result on unique decomposition.

(4) $v_p(1) = 0$ since 1 is a unit. □

Proposition – $\mathbb{Z}_p$ Integral Domain

For all $x, y \in \mathbb{Z}_p$, $xy = 0$ implies $x = 0$ or $y = 0$.

Proof. Follows from the norm being multipicative and $\mathbb{R}$ being an integral domain. □

Proof. (Without using the norm)

Let $x, y \in \mathbb{Z}_p$, $x \neq 0 \neq y$. Then $xy = p^{v_p(x)+v_p(y)}u(x)u(y)$ from unique decomposition. Then $xy = 0$ yields $0 = p^{v_p(x)+v_p(y)}$, which implies $\mathbb{Z}$ does not inject into $\mathbb{Z}_p$, a contradiction. $\square$

> **Proposition – Ultrametric Property**
> Let (X, d) be a metric space with d satisfying the *ultrametric property* : for all $x, y, z \in X$, $d(x, z) \leq \max(d(x, y), d(y, z))$. Then for all sequences $a : \mathbb{N} \to X$, a_n is cauchy if and only if $\lim_{n\to\infty} d(a_n, a_{n+1}) = 0$.

Proof. Elementary. $\square$

> **Proposition – Topological Properties of $\mathbb{Z}_p$**
> The following are true :
>
> 1. (Topology) For each $x \in \mathbb{Z}_p$, the set of balls $\left\{B_{p^{-n}(x)}\right\}_{n\in\mathbb{N}}$ is a prefilter that generates the neighbourhood filter of x under the subspace topology of $\mathbb{Z}_p$ in $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ with the product topology from each $\mathbb{Z}/p^n\mathbb{Z}$ being discrete. That is to say, the topology from the norm is equal to the topology from the construction of $\mathbb{Z}_p$.
> 2. (Completeness) $\mathbb{Z}_p$ is compact. Hence a complete metric space under $|\star|_p$.
> 3. (Density of $\mathbb{Z}$ in $\mathbb{Z}_p$) For each $x \in \mathbb{Z}_p$, there exists unique $a : \mathbb{N} \to \{0, \dots, p-1\}$ such that $x = \sum_{k=0}^{\infty} a_k p^k$. Furthermore, for all $a : \mathbb{N} \to \{0, \dots, p-1\}$, $\sum_{k=0}^{\infty} a_k p^k$ is convergent in $\mathbb{Z}_p$.

Proof.

(1) Let $x \in \mathbb{Z}_p$. By the definition of product topology, the neighbourhood filter of x is generated by the set of preimages of open neighbourhoods of $\varepsilon_n(x)$, where n ranges over $\mathbb{N}$. Since the $\mathbb{Z}/p^n\mathbb{Z}$ are all discrete, the neighbourhood filter of x is generated by the smaller set of $\left\{\varepsilon_n^{-1}(\varepsilon_n(x))\right\}_{n\in\mathbb{N}} = \{x + p^n\mathbb{Z}_p\}_{n\in\mathbb{N}} = \left\{B_{p^{-n+1}}(x)\right\}_{n\in\mathbb{N}}$, hence the result.

(2) Define $C : \mathbb{N} \to 2^{\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}}$ by mapping $n \in \mathbb{N}$ to the set of elements x such that $\downarrow_n^{n+1} \varepsilon_{n+1}(x) = \varepsilon_n(x)$. Then $\mathbb{Z}_p = \bigcap_{n\in\mathbb{N}} C_n$. Since $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ is compact by Tychonoff's theorem and closed in compact implies compact, it suffices to show that each C_n is closed. We can describe C_n explicitly as

$$C_n = \bigcup_{y\in\mathbb{Z}/p^n\mathbb{Z}} \bigcup_{z\in\left(\downarrow_n^{n+1}\right)^{-1}y} \varepsilon_n^{-1}y \cap \varepsilon_{n+1}^{-1}z$$

Since every $\mathbb{Z}/p^n\mathbb{Z}$ is discrete, this is a finite union of closed sets and hence is closed.

(3) In the following, let $\pi_k : \mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ be the natural map. Let $x \in \mathbb{Z}_p$. For $k \in \mathbb{N}$, let $x_k \in \mathbb{Z}$ be unique such that $\pi_k(x_k) = \varepsilon_k(x)$ and $0 \leq x_k < p^k$. There exists a unique $a^{(k)} : \mathbb{N} \to \{0, \dots, p-1\}$ such that $x_k = \sum_{l\in\mathbb{N}} a_l^{(k)} p^l$. Since $\pi_k(x_{k+1} - a^{(k+1)}(k)p^k) = \pi_k(x_{k+1}) =\downarrow_k^{k+1} \varepsilon_{k+1}(x) = \varepsilon_k(x) = x_k$ and $0 \leq x_{k+1} - a^{(k+1)}(k)p^k < p^k$, we have $x_{k+1} = x_k + a^{(k+1)}(k)p^k$. Therefore $a : \mathbb{N} \to \{0, \dots, p-1\}, k \mapsto a^{(k)}(k)$. The claim that $x = \sum_{k=0}^{\infty} a_k p^k$ is equivalent to $x = \lim_{k\to\infty} x_k$. Since the neighourhood filter of x is generated

by $B_{p^{-n}}(x)$, it suffices x_k converges into each of these balls. Let $n \in \mathbb{N}$. Then for $k \geq n+1$, $\varepsilon_{n+1}(x_k - x) =\downarrow_{n+1}^{k} \varepsilon_k(x_k - x) = 0$. Therefore $n < v_p(x_k - x)$, i.e. $x_k \in B_{p^{-n}}(x)$. Hence, $x_k \to x$.

Let $b : \mathbb{N} \to \{0, \ldots, p-1\}$ such that $x = \sum_{k=0}^{\infty} b_k p^k$. Then $\pi_1(a_0) = \varepsilon_1(x) = \pi_1(b_0)$. Since $0 \leq a_0, b_0 < p$, $a_0 = b_0$. For $k \in \mathbb{N}$, $\pi_{k+1}(a_k p^k) = \varepsilon_{k+1}(x - \sum_{0 \leq l < k} a_l p^l) = \varepsilon_{k+1}(x - \sum_{0 \leq l < k} b_l p^l) = \pi_{k+1}(b_k p^k)$ by induction. Since $0 \leq a_k, b_k < p$, $a_k p^k = b_k p^k$ and hence $a_k = b_k$. Therefore $a = b$.

A general power series in p converges because $\left|a_k p^k\right|_p \leq |p|_p^k = p^{-k} \to 0$, the ultrametric property of the norm and completeness of $\mathbb{Z}_p$. ☐

Definition – p-adic Rationals

$\mathbb{Q}_p$ is defined as the field of fractions of $\mathbb{Z}_p$.

Proposition – $\mathbb{Q}_p$ as Localizing $\mathbb{Z}_p$ at p

As $\mathbb{Z}_p$ algebras, $\mathbb{Q}_p$ is canonically isomorphic to $(\mathbb{Z}_p)_p = \mathbb{Z}_p[X]/(pX-1)\mathbb{Z}_p[X]$, the localization of $\mathbb{Z}_p$ with respect to the element p.

Proof. Since p is invertible in $\mathbb{Q}_p$, there is a canonical $\mathbb{Z}_p$-algebra morphism from $(\mathbb{Z}_p)_p$ to $\mathbb{Q}_p$. Since $\mathbb{Z}_p$ be an integral domain, $\mathbb{Z}_p$ injects into $\mathbb{Q}_p$ and thus $(\mathbb{Z}_p)_p$ injects into $\mathbb{Q}_p$ as well. By unique decomposition, every element of $\mathbb{Q}_p$ is of the form $(p^n u)/(p^m v)$ where $n, m \in \mathbb{N}$ and $u, v \in \mathbb{Z}_p^\times$. Therefore every element of $\mathbb{Q}_p$ is of the form $p^k w$ where $k \in \mathbb{Z}$ and $w \in \mathbb{Z}_p^\times$. This shows $(\mathbb{Z}_p)_p$ surjects onto $\mathbb{Q}_p$, i.e. the canonical morphism from $(\mathbb{Z}_p)_p$ to $\mathbb{Q}_p$ is an isomorphism. ☐

Remark – Meaning of $\mathbb{Q}_p$. Continuing with the analogy, $\mathbb{Q}_p$ is the field of Laurent series at p with p as a non-essential singularity.

Definition – p-adic Valuation on $\mathbb{Q}_p$

We extend the p-adic valuation to $\mathbb{Q}_p$ by :

$$v_p : \mathbb{Q}_p \to \mathbb{N}^\infty, \frac{x}{p^n} \in (\mathbb{Z}_p)_p \mapsto v_p(x) - n$$

From this, we extend the p-adic norm as well :

$$|\star|_p : \mathbb{Q}_p \to [0, \infty) \subseteq \mathbb{R}, x \mapsto \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0 \end{cases}$$

Proposition – Topological Properties of $\mathbb{Q}_p$

The following are true :

1. $(\mathbb{Q}_p, |\star|_p)$ is a normed ring (field) and hence a topological ring.
2. $\mathbb{Z}_p$ is homeomorphic to its canonical image in $\mathbb{Q}_p$, where it is an open subring of $\mathbb{Q}_p$. Hence, $\mathbb{Q}_p$ is locally compact.
3. $\mathbb{Q}_p$ is complete.

4. Since $\mathbb{Z}$ injects canonically into $\mathbb{Q}_p$, $\mathbb{Q}$ injects canonically into $\mathbb{Q}_p$ as well. Then $\mathbb{Q}$ is dense $\mathbb{Q}_p$.

Proof.

(1) Same proof as for $\mathbb{Z}_p$.

(2) Since the norm of $\mathbb{Q}_p$ extends that of $\mathbb{Z}_p$, $\mathbb{Z}_p$ is homeomorphic to its canonical image in $\mathbb{Q}_p$. $\mathbb{Z}_p = B_p(0)$, since the image of $|\star|_p$ is discrete. For all points $x \in \mathbb{Q}_p$, the clopen ball of size 1 around x is homeomorphic to $\mathbb{Z}_p$ (by translation). Hence every x has a compact neighbourhood.

(3) Let $a : \mathbb{N} \to \mathbb{Q}_p$ be a cauchy sequence. Then there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $a_n \in B_1(a_N) = a_N + \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is complete and $B_1(a_N)$ is isometric to $\mathbb{Z}_p$, a_n converges in $B_1(a_N)$ and hence in $\mathbb{Q}_p$.

(4) follows from elements in $\mathbb{Q}_p$ being of the form $p^{-n}x$ where $x \in \mathbb{Z}_p$ and $\mathbb{Z}$ being dense in $\mathbb{Z}_p$. $\square$

1.2 p-adic Equations

Proposition – Inverse Limit of Finite, Non-Empty System is Non-Empty

Let $D : \mathbb{N}^{op} \to \mathbf{Set}$ be a projective system such that for all $n \in \mathbb{N}$, D_n is finite and non-empty. Then $\varprojlim n \in \mathbb{N}^{op} D_n$ is nonempty.

Proof. If D is a surjective system, then $\varprojlim n \in \mathbb{N} D_n$ is non-empty. We will reduce to this case.

For $n \in \mathbb{N}$, consider the descending sequence of subsets $\left\{\downarrow_n^k D_k \,|\, n \leq k\right\}$ in D_n. Since D_n is finite, there exists an N such that for all $k \geq N$, $\downarrow_n^k D_k = \downarrow_n^N D_N$. For $n \in \mathbb{N}$, let $N(n)$ be the minimal natural with respect to this property. Let $E_n := \downarrow_n^{N(n)} D_{N(n)}$. Since $D_{N(n)} \neq \varnothing$, $E_n \neq \varnothing$. For $n \in \mathbb{N}$, let $M = \max(N(n), N(n+1))$. Then $E_n = \downarrow_n^M D_M = \downarrow_n^{n+1} \downarrow_{n+1}^M D_M = \downarrow_n^{n+1} E_{n+1}$. Thus $E : \mathbb{N}^{op} \to \mathbf{Set}$ is a non-empty, surjective system that injects into D. Therefore $\varnothing \neq \varprojlim n \in \mathbb{N}^{op} E_n \to \varprojlim n \in \mathbb{N}^{op} D_n$. $\square$

Notation. Let $n \in \mathbb{N}, 0 < m$. Then there is a canonical morphism of $\mathbb{Z}_p$ algebras from $\mathbb{Z}_p[X_1, \ldots, X_m]$ to $\mathbb{Z}/p^n\mathbb{Z}[X_1, \ldots, X_m]$. For $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, let f_n denote its image in $\mathbb{Z}/p^n\mathbb{Z}[X_1, \ldots, X_m]$. More explicitly, for $f = \sum_{t \in \mathbb{N}^m} a_t \underline{X}^t$,

$$f_n := \sum_{t \in \mathbb{N}^m} \varepsilon_n(a_t) \underline{X}^t$$

Proposition – p-adic Affine Variety is Inverse Limit

Let $0 < m$, $I \subseteq \mathbb{Z}_p[X_1, \ldots, X_m]$, I_n the image of I in $\mathbb{Z}/p^n\mathbb{Z}[X_1, \ldots, X_m]$ for $n \in \mathbb{N}$. Then $\mathbb{V}I \cong \varprojlim n \in \mathbb{N}^{op} \mathbb{V}I_n$ as sets. In particular, the variety defined by I is non-empty if and only if for all $n \in \mathbb{N}$, its projection mod p^n is non-empty.

Proof. We first show that $\mathbb{Z}_p^m$ has the universal property of $\varprojlim n \in \mathbb{N}^{op} (\mathbb{Z}/p^n\mathbb{Z})^m$. Let X be an arbitrary set. We have the following chain of set-theoretic isomorphisms :

$$\mathbf{Set}(X, \mathbb{Z}_p^m) \cong (\mathbf{Set}(X, \mathbb{Z}_p))^m \cong \left(\mathbf{Set}^{\mathbb{N}^{op}}(\underline{X}, \mathbb{Z}/p^\star\mathbb{Z})\right)^m \cong \mathbf{Set}^{\mathbb{N}^{op}}(\underline{X}, (\mathbb{Z}/p^\star\mathbb{Z})^m)$$

Thus $\mathbb{Z}_p^m \cong \varprojlim n \in \mathbb{N}^{op} (\mathbb{Z}/p^n\mathbb{Z})^m$ in a unique way that commutes with their projections to $(\mathbb{Z}/p^n\mathbb{Z})^m$.

For $x \in \mathbb{Z}_p^m$ and $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $f(x) = 0$ if and only if for all $n \in \mathbb{N}$, $\varepsilon_n \circ f(x) = 0$. For $n \in \mathbb{N}$,

$$\varepsilon_n \circ f(x) = \varepsilon_n \left(\sum_{t \in \mathbb{N}^m} a_t x^t \right) = \sum_{t \in \mathbb{N}^m} \varepsilon_n(a) \varepsilon_n^m(x)^t = f_n \circ \varepsilon_n^m(x)$$

Therefore $f(x) = 0$ if and only if for all $n \in \mathbb{N}$, $f_n \circ \varepsilon_n^m(x) = 0$. This shows that $\mathbb{V}I \cong \varprojlim n \in \mathbb{N}^{op} \mathbb{V}I_n$ under the isomorphism $\mathbb{Z}_p^m \cong \varprojlim n \in \mathbb{N}^{op} (\mathbb{Z}/p^n\mathbb{Z})^m$.

The 'in particular' follows from inverse limit of finite, nonempty is nonempty. $\square$

Definition – Primitive Solutions

Let $m, n \in \mathbb{N}^+$. For $x \in \mathbb{Z}_p^m$, x is called *primitive* when $\varepsilon_1^m(x) \neq 0$, i.e. when it is not divisible by p. Similarly, for $x \in (\mathbb{Z}/p^n\mathbb{Z})^m$, x is called primitive when $(\downarrow_1^n)^m x \neq 0$.

Definition – Homogeneous Polynomials

Let $1 \leq m$, A be a commutative ring, $f \in A[X_1, \ldots, X_m]$. Then f is called *homogeneous* when for all $\lambda \in A$, $f(\lambda X) = \lambda^{\deg f} f(X)$. Equivalently, all monomials in f with non-zero coefficients have the same degree.

Proposition – $\mathbb{Q}_p$, $\mathbb{Z}_p$ Points of Projective Varieties(?)

Let $1 \leq m$, $I \subseteq \mathbb{Z}_p[X_1, \ldots, X_m]$, for all $f \in I$, f homogeneous. Then the following are equivalent :

1. There exists $x \in \mathbb{V}[\mathbb{Q}_p]I$ such that $x \neq 0$.
2. There exists $x \in \mathbb{V}[\mathbb{Z}_p]I$ such that x is primitive.
3. For all $n \geq 1$, there exists $x_n \in \mathbb{V}[\mathbb{Z}/p^n\mathbb{Z}]I_n$ such that x_n primitive. [a]

[a] Serre only requires $n > 1$. This is indeed equivalent since have a primitive zero for any $n > 1$ automatically gives you a primitive zero for $n = 1$ via $\downarrow_1^n$. We cannot let $n = 0$ though, since there are no primitive elements in $\mathbb{Z}/\mathbb{Z}^m = 0^m$.

Proof.

($1 \Leftrightarrow 2$) The reverse implication is clear. For forwards, let $x = (x_i)_{i=1}^m \in \mathbb{V}[\mathbb{Q}_p]I$, $x \neq 0$. Let $h := \inf \{v_p(x_i) \mid i = 1, \ldots, m\}$. Since $x \neq 0$, $h < \infty$. Let $y := p^{-h}x$. Then by definition of h, $y \in \mathbb{Z}_p^m$ and there exists one component that is not-divisible by p, i.e. y is primitive. Then $f(y) = p^{-h \deg f} f(x) = 0$ by homogeneity of f. Thus y is as desired.

($2 \Leftrightarrow 3$) It suffices to show that the sets of primitive elements in $\mathbb{V}[\mathbb{Z}/p^n\mathbb{Z}]I_n$ forms a projective subsystem of $\mathbb{V}[\mathbb{Z}/p^\star\mathbb{Z}]I_\star$ and that the inverse limit is isomorphic to the primitive elements in $\mathbb{V}[\mathbb{Z}_p]I$.

Let $P : \mathbb{N}^{op} \to \mathbf{Set}$, $n \mapsto \mathbb{V}[\mathbb{Z}/p^n\mathbb{Z}]I_n \cap \{x \mid x \text{ primitive}\}$. By the definition of $\mathbb{V}[\mathbb{Z}/p^\star\mathbb{Z}]I_\star$ being projective, ${\downarrow_n^{n+1}}^m$ takes primitive zeros to primitive zeros. This induces the structure of a projective system for P, making it a subsystem of $\mathbb{V}[\mathbb{Z}/p^\star\mathbb{Z}]I_\star$. Hence, $\varprojlim n \in \mathbb{N}^{op} P_n$ injects into $\mathbb{V}[\mathbb{Z}_p]I$ canonically. We identify it with its image. Clearly, for any $x \in \varprojlim n \in \mathbb{N}^{op} P_n$, $\varepsilon_1(x) \neq 0$. So $\varprojlim n \in \mathbb{N}^{op} P_n$ is a subset of primitive elements of $\mathbb{V}[\mathbb{Z}_p]I$. Conversely, any primitive element x of $\mathbb{V}[\mathbb{Z}_p]I$ defines a natural transformation from the singleton set $*$ as a constant functor to the projective system P, i.e. an element of $\varprojlim n \in \mathbb{N}^{op} P_n$ that maps to x. Hence $\varprojlim n \in \mathbb{N}^{op} P_n$ is equal to the set of primitives in $\mathbb{V}[\mathbb{Z}_p]I$. $\square$

Remark – Goal of this section. To give conditions to lift approximate solutions mod p^n to solutions in $\mathbb{Z}_p$. This will be done via the p-adic analogue of Newton's method. As with Newton's method from real analysis, we need mean value theorem.

> **Proposition – Mean Value Theorem for Polynomials**
> Let A be a commutative ring, $f \in A[X]$, $a \in A$. Then $f - f(a) = f'(a)(X-a)$ in $A[X]/(X-a)^2 A[X]$.

Proof. If the result is true for $g, h \in A[X]$, then it's true for $\lambda g + h$ where $\lambda \in A$. Therefore it suffices to show the result for monomial X^n. This follows from induction. $\square$

> **Proposition – p-adic Newton's Method**
> Let $f \in \mathbb{Z}_p[X]$, $x \in \mathbb{Z}_p$ such that
> $$|f(x)|_p < |f'(x)|_p^2$$
> Then there exists $\overline{x} \in \mathbb{Z}_p$ such that
> 1. $|f(\overline{x})|_p \leq p^{-1} |f(x)|_p$
> 2. $|\overline{x} - x|_p \leq \frac{|f(x)|_p}{|f'(x)|_p}$
> 3. $|f'(\overline{x})|_p = |f'(x)|_p$

Proof. If $f(x) = 0$, then pick $\overline{x} = x$. So WLOG $0 < |f(x)|_p$. Note that since all p-adic integers have norm ≤ 1, we have $|f(x)|_p < |f'(x)|_p$. Then $1 < |f'(x)|_p |f(x)|_p^{-1} \in p\mathbb{Z} \subseteq p\mathbb{Z}_p$. Define

$$\overline{x} := x + \frac{|f'(x)|_p}{|f(x)|_p} y$$

for some $y \in \mathbb{Z}_p$ to be determined. Then by applying mean value theorem to f, we have

$$\begin{aligned} f(\overline{x}) &= f(x) + f'(x)(\overline{x} - x) + a_0(\overline{x} - x)^2 \\ &= f(x) + f'(x) y |f'(x)|_p |f(x)|_p^{-1} + a |f'(x)|_p^2 |f(x)|_p^{-2} \end{aligned}$$

for some $a, a_0 \in \mathbb{Z}_p$. By definition of $|\star|_p$, the topology of $\mathbb{Z}_p$ and unique decomposition, $f(x) = b |f(x)|_p^{-1}$ for some $b \in \mathbb{Z}_p^\times$ and $f'(x) = c |f'(x)|_p^{-1}$ for some $c \in \mathbb{Z}_p^\times$. We thus have

$$f(\overline{x}) = (b + yc) |f(x)|_p^{-1} + a |f'(x)|_p^2 |f(x)|_p^{-2}$$

Choosing $y := -bc^{-1}$, we obtain :

$$\begin{aligned} &|f(\overline{x})|_p = \left| a |f'(x)|_p^2 |f(x)|_p^{-2} \right|_p \leq |f(x)|_p^2 |f'(x)|_p^{-2} < |f(x)|_p \Rightarrow |f(\overline{x})|_p \leq p^{-1} |f(x)|_p \\ &|f'(x)|_p |\overline{x} - x|_p = \left| f(\overline{x}) - f(x) - a_0(\overline{x} - x)^2 \right|_p \leq \max(|f(\overline{x})|_p, |f(x)_p|, \left|a_0(\overline{x} - x)^2\right|_p) = |f(x)|_p \end{aligned}$$

It remains to show $|f'(\overline{x})|_p = |f'(x)|_p$. By applying mean value theorem to f', we have for some $d, e \in \mathbb{Z}_p$,

$$\begin{aligned} f'(\overline{x}) &= f'(x) + f''(x)y\,|f'(x)|_p\,|f(x)|_p^{-1} + d\,|f'(x)|_p^2\,|f(x)|_p^{-2} \\ &= |f'(x)|_p^{-1}\left(c + e\,|f'(x)|^2\,|f(x)|_p^{-1} + d\,|f'(x)|_p^3\,|f(x)|_p^{-2}\right) \end{aligned}$$

Since $\left|e\,|f'(x)|^2\,|f(x)|_p^{-1}\right|_p \leq |f(x)|\,|f'(x)|_p^{-2} < 1$ and $\left|d\,|f'(x)|_p^3\,|f(x)|_p^{-2}\right|_p \leq |f(x)|_p^2\,|f'(x)|_p^{-4} < 1$, the term being multiplied by $|f'(x)|_p^{-1}$ is still a unit, and hence norm 1. It then follows from taking norms that $|f'(\overline{x})|_p = \left||f'(x)|_p^{-1}\right|_p = |f'(x)|_p$. $\square$

> **Proposition – Lifting Solutions / Generalized Hensel's Lemma**
> Let $1 \leq m$, $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x \in \mathbb{Z}_p^m$ such that there exists $1 \leq j \leq m$ satisfying
>
> $$|f(x)|_p < \left|\left.\frac{\partial f}{\partial X_j}\right|_x\right|_p^2$$
>
> Then there exists $y \in \mathbb{Z}_p^m$ such that $f(y) = 0$ and
>
> $$\max(|\pi_i(y - x)|_p)_{1 \leq i \leq m} \leq \frac{|f(x)|_p}{\left|\left.\frac{\partial f}{\partial X_j}\right|_x\right|_p}$$
>
> where $\pi_i : \mathbb{Z}_p^m \to \mathbb{Z}_p$ takes the i-th component.

Proof. We induct on m.

Suppose $m = 1$. Define $x_0 := x$. Then $|f(x_0)|_p < |f'(x_0)|_p^2$, so by p-adic Newton's method, we have $x_1 \in \mathbb{Z}_p$ such that

1. $|f(x_1)|_p \leq p^{-1}\,|f(x_0)|_p$
2. $|x_1 - x_0|_p \leq \frac{|f(x_0)|_p}{|f'(x_0)|_p}$
3. $|f'(x_1)|_p = |f'(x_0)|_p$

Then $|f(x_1)|_p < |f'(x_1)|_p^2$. By induction, we have a sequence $x : \mathbb{N} \to \mathbb{Z}_p$ such that for all $k \in \mathbb{N}$,

1. $|f(x_{k+1})|_p \leq p^{-1}\,|f(x_k)|_p \leq p^{-(k+1)}\,|f(x_0)|_p$
2. $|x_{k+1} - x_k|_p \leq \frac{|f(x_k)|_p}{|f'(x_k)|_p} \leq \frac{|f(x_0)|_p}{p^k|f'(x_0)|_p}$
3. $|f'(x_{k+1})|_p = |f'(x_k)|_p$

From (1), we see that $\lim_{k\to\infty} f(x_k) = 0$. From (2) and the ultrametric property of $|\star|_p$, there exists $y \in \mathbb{Z}_p$ such that $\lim_{k\to\infty} x_k = y$. Since $\mathbb{Z}_p$ is a topological ring with topology from $|\star|_p$ and the map $\mathbb{Z}_p \to$

$\mathbb{Z}_p, x \mapsto f(x)$ is defined by finitely many additions and multiplications, it is continuous and hence $f(y) = f(\lim_{k\to\infty} x_k) = \lim_{k\to\infty} f(x_k) = 0$. For $k \in \mathbb{N}$, again by the ultrametric property,

$$|x_k - x|_p \leq \max\left(|x_0 - x|_p, \ldots, |x_k - x|_p\right) \leq \frac{|f(x_0)|_p}{|f'(x_0)|_p}$$

Taking limits, we obtain

$$|y - x|_p \leq \frac{|f(x_0)|_p}{|f'(x_0)|_p}$$

as desired.

For $1 < m$, we reduce to the single variable case. Define $\overline{f}(X_j) := f(\pi_1(x), \ldots, X_j, \ldots, \pi_m(x)) \in \mathbb{Z}_p[X_j]$. By the single variable case, there exists $y_j \in \mathbb{Z}_p$ such that $\overline{f}(y_j) = 0$ and

$$|y_j - \pi_j(x)|_p \leq \frac{\left|\overline{f}(\pi_j(x))\right|_p}{\left|\overline{f}'(\pi_j(x))\right|_p} = \frac{|f(x)|_p}{|f'(x)|_p}$$

Let $y = (\pi_1(x), \ldots, y_j, \ldots, \pi_m(x)) \in \mathbb{Z}_p^m$. Then $f(y) = \overline{f}(y_j) = 0$ and for all $1 \leq i \leq m$,

$$|\pi_i(y - x)|_p \begin{cases} = 0 & i \neq j \\ \leq \frac{|f(x)|_p}{|f'(x)|_p} & i = j \end{cases}$$

□

> **Proposition – Hensel's Lemma**
> Let $1 \leq m$, $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x \in \mathbb{Z}_p^m$, $\varepsilon_1(f(x)) = 0$, $1 \leq i \leq m$, $\varepsilon_1(\frac{\partial f}{\partial X_i}\Big|_x) \neq 0$. Then there exists $y \in \mathbb{Z}_p^m$ such that $f(y) = 0$ and $\varepsilon_1^m(y - x) = 0$.

Proof. $\varepsilon_1(f(x)) = 0$ is equivalent to $|f(x)|_p \leq p^{-1}$ and $\varepsilon_1(\frac{\partial f}{\partial X_i}\Big|_x) \neq 0$ is equivalent to $\left|\frac{\partial f}{\partial X_i}\Big|_x\right|_p = 1$. The conditions of lifting solutions are satisfied, hence we have $y \in \mathbb{Z}_p^m$ such that for all $1 \leq i \leq m$,

$$\max(|\pi_i(y - x)|_p)_{1 \leq i \leq m} \leq \frac{|f(x)|_p}{\left|\frac{\partial f}{\partial X_j}\Big|_x\right|_p}$$

The inequality is equivalent to $\varepsilon_1^m(y - x) = 0$. □

> **Proposition – Lifting Solutions of Quadratic Forms for $p \neq 2$**
> Let $p \neq 2$, $1 \leq m$, $f = \sum_{i,j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \ldots, X_m]$ where
>
> 1. $[a_{ij}]^\top = [a_{ij}]$
> 2. $\det[a_{ij}] \in \mathbb{Z}_p^\times$

i.e. f is a non-degenerate quadratic form. Let $a \in \mathbb{Z}_p$, $x \in \mathbb{Z}_p^m$ such that x is primitive and $\varepsilon_1(f(x)) = \varepsilon_1(a)$. Then there exists $y \in \mathbb{Z}_p^m$ such that $f(y) = a$ and $\varepsilon_1^m(y - x) = 0$.

Proof. By Hensel's Lemma, it suffices to give $1 \leq i \leq m$ such that $\varepsilon_1(\frac{\partial f}{\partial X_i}\Big|_x) \neq 0$. Taking the derivative of f, evaluating at x and reducing mod p yields the following linear system :

$$\left[\varepsilon_1\left(\frac{\partial f}{\partial X_i}\bigg|_x\right)\right]_{i=1}^m = 2[\varepsilon_1(a_{ij})]_{i,j=1}^m \varepsilon_1(x)$$

Since $\det[a_{ij}] \in \mathbb{Z}_p^\times$, $\det[\varepsilon_1(a_{ij})]_{i,j=1}^m \neq 0$. The matrix is hence invertible and since $\varepsilon_1(x) \neq 0$ by definition of primitivity, there exists a desired $1 \leq i \leq m$. ☐

Proposition – Lifting Solutions of Quadratic Forms for $p = 2$
Let $p = 2$, $1 \leq m$, $f = \sum_{i,j=1}^m a_{ij} X_i X_j \in \mathbb{Z}_p[X_1, \ldots, X_m]$ where $[a_{ij}]^\top = [a_{ij}]$, i.e. f is a quadratic form. Let $a \in \mathbb{Z}_2$, $x \in \mathbb{Z}_2^m$ such that x is primitive and $\varepsilon_3(f(x)) = \varepsilon_3(a)$. Then

1. Let $1 \leq i \leq m$ where $\varepsilon_2\left(\frac{\partial f}{\partial X_i}\Big|_x\right) \neq 0$. Then there exists $y \in \mathbb{Z}_2^m$ such that $f(y) = a$ and $\varepsilon_3(y - x) = 0$.
2. The condition of (1) is satisfied when $\det[a_{ij}]_{i,j=1}^m \in \mathbb{Z}_2^\times$.

Proof.

(1) $\varepsilon_3(f(x)) = \varepsilon_3(a)$ and $\varepsilon_2\left(\frac{\partial f}{\partial X_i}\Big|_x\right) \neq 0$ are respectively equivalent to $|f(x) - a|_p \leq p^{-3}$ and $p^{-1} \leq \left|\frac{\partial f}{\partial X_i}\Big|_x\right|_p$. Hence

$$|f(x) - a|_p < \left|\frac{\partial f}{\partial X_i}\bigg|_x\right|_p^2$$

So by lifting solutions, there exists $y \in \mathbb{Z}_p^m$ such that $f(y) = a$ and

$$\max(|\pi_i(y - x)|_p)_{1 \leq i \leq m} \leq \frac{|f(x) - a|_p}{\left|\frac{\partial f}{\partial X_j}\Big|_x\right|_p}$$

By taking the derivative of f, evaluating at x and reducing mod 2, we have $\varepsilon_1\left(\frac{\partial f}{\partial X_i}\Big|_x\right) = 0$ and hence its valuation is 1. We thus obtain

$$\max(|\pi_i(y - x)|_p)_{1 \leq i \leq m} \leq p^{-2}$$

This is equivalent to $\varepsilon_2(y - x) = 0$.

(2) This follows from taking the derivative of f, reducing mod 4 and using the primitivity of x and invertibility of $\varepsilon_2[a_{ij}]_{i,j=1}^m$. ☐

1.3 Units of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

Definition – Group Ring

Let G be an abelian group. Then the *group ring over G* is defined as

$$\mathbb{Z}[G] := \mathbb{Z}[X_g]_{g\in G}/I$$

where $I := (X_e - 1)\mathbb{Z}[X_g]_{g\in G} + \sum_{g,h\in G}(X_gX_h - X_{gh})\mathbb{Z}[X_g]_{g\in G}$.

Notation. For G an abelian group, $g \in G$, we denote the image of X_g in $\mathbb{Z}[G]$ with g. So elements of $\mathbb{Z}[G]$ are formal polynomials in elements of G such that multiplication respects the multiplication of G. With this, G injects into $\mathbb{Z}[G]$ and we subsequently identify G with its image in $\mathbb{Z}[G]$.

Proposition – Adjunction of Group Rings and Units

The following are true :

1. $\mathbb{Z}[-] : \mathbf{Ab} \to \mathbf{CRing}$ is a functor.

2. $\mathbb{Z}[-]$ and $(-)^\times$ forms an adjunction, that is to say $\mathbf{CRing}(\mathbb{Z}[-],\star) \cong \mathbf{Ab}(-,(\star)^\times)$ naturally.

Proof. (1) Follows from the universal property of polynomial ring over a set and quotient ring.

(2) For a commutative ring A and abelian group G, the map is $\mathbf{CRing}(\mathbb{Z}[G], A) \to \mathbf{Ab}(G, A\times), f \mapsto f(g)$. This is well-defined because $G \subseteq \mathbb{Z}[G]^\times$. Injectivity and surjectivity follows, again, from universal property of the polynomial ring over G and quotient ring. Naturality is straightforward to check. $\square$

Proposition – Coprime implies Split Exact

Let $0 \to A \to E \to B \to 0$ be a short exact sequence of abelian groups. Let $a = |A|, b = |B|, a, b < \infty$ such that a, b coprime. Let $B' := \ker(b : x \mapsto bx)$. Then $E \cong A \oplus B'$ canonically and B' is the unique subgroup of E isomorphic to B.

Proof. Elementary. $\square$

In the following subsection, let $\mathbb{U} := \mathbb{Z}_p^\times$ and for $n \in \mathbb{N}$, $\mathbb{U}_n := \ker((\varepsilon_n)^\times : \mathbb{U} \to \mathbb{Z}/p^n\mathbb{Z}^\times)$.

Proposition – Units of $\mathbb{Z}_p$ as a Inverse Limit

$\mathbb{U}$ is a inverse limit of the projective system $\mathbb{U}/\mathbb{U}_\star$ in the category of abelian groups. More generally, for $k \in \mathbb{N}$, $\mathbb{U}_k \cong \varprojlim \mathbb{U}_k/\mathbb{U}_{k+\star}$ canonically.

Proof. From truncation, we have $\mathbb{Z}_p/p^\star\mathbb{Z}_p \cong \mathbb{Z}/p^\star\mathbb{Z}$ canonically as projective systems of commutative rings. By taking inverse limits, we see that $\varprojlim \mathbb{Z}_p/p^\star\mathbb{Z}_p \cong \mathbb{Z}_p$ canonically. The result now follows since taking units is a right adjoint functor, and hence preserves limits.

Now let $k \in \mathbb{N}$. Consider the following short exact sequence of projective systems of abelian groups :

$$1 \to \mathbb{U}_k/\mathbb{U}_\star \to \mathbb{U}/\mathbb{U}_\star \to \underline{\mathbb{U}/\mathbb{U}_k} \to 1$$

where

$$\mathbb{U}_k/\mathbb{U}_\star : n \in \mathbb{N}^{op} \mapsto \begin{cases} 1 & , n \leq k \\ \mathbb{U}_k/\mathbb{U}_n & , k \leq n \end{cases}$$

and

$$\underline{\mathbb{U}/\mathbb{U}_k} : n \in \mathbb{N}^{op} \mapsto \begin{cases} 1 & , n \leq k \\ \mathbb{U}/\mathbb{U}_k & , k \leq n \end{cases}$$

The sequence is short exact by the 3rd isomorphism theorem for groups. Since the system $\mathbb{U}_k/\mathbb{U}_\star$ is surjective, we can pass the short exact sequence to the inverse limit and obtain the short sequence of abelian groups :

$$1 \to \varprojlim \mathbb{U}_k/\mathbb{U}_\star \to \mathbb{U} \to \mathbb{U}/\mathbb{U}_k \to 1$$

This shows that $\mathbb{U}_k \cong \varprojlim \mathbb{U}_k/\mathbb{U}_\star \cong \varprojlim \mathbb{U}_k/\mathbb{U}_{k+\star}$ canonically as abelian groups. □

> **Proposition – The order of $\mathbb{U}_k/\mathbb{U}_n$**
> Let $n \in \mathbb{N}$. Then $U_n/U_{n+1} \cong \ker\left(\downarrow_n^{n+1}\right)^\times$ canonically as abelian groups, which is in turn isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Hence for $k \geq n$, $|U_k/U_n| = p^{n-k}$.

Proof. Consider the following commutative diagram :

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{U}_{n+1} \arrow[r] \arrow[d, "\subseteq"] & \mathbb{U} \arrow[r] \arrow[d, "\mathbb{1}"] & \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times \arrow[r] \arrow[d, "(\downarrow_n^{n+1})^\times"] & 1 \\ 1 \arrow[r] & \mathbb{U}_n \arrow[r] & \mathbb{U} \arrow[r] & (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r] & 1 \end{tikzcd}$$

Then by the snake lemma, we have the exact sequence :

$$1 \to 1 \to 1 \to \ker\left(\downarrow_n^{n+1}\right)^\times \to \mathbb{U}_n/\mathbb{U}_{n+1} \to 1 \to 1 \to 1$$

which says $U_n/U_{n+1} \cong \ker\left(\downarrow_n^{n+1}\right)^\times$. By counting $\left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times$ and $(\mathbb{Z}/p^n\mathbb{Z})^\times$, we obtain $\left|\ker\left(\downarrow_n^{n+1}\right)^\times\right| = p$ and hence isomorphic to $\mathbb{Z}/p\mathbb{Z}$ since p is prime. To show $|U_k/U_n| = p^n$ for $n \leq k$, note that by the first isomorphism, $\mathbb{U}_k/\mathbb{U}_{n-1} \cong (\mathbb{U}_k/\mathbb{U}_n)/(\mathbb{U}_n/\mathbb{U}_{n-1})$, so $|\mathbb{U}_k/\mathbb{U}_n| = |\mathbb{U}_n/\mathbb{U}_{n-1}|\,|\mathbb{U}_k/\mathbb{U}_{n-1}| = p^{n-k}$ by induction. □

> **Proposition – Structure of $\mathbb{U}$**
> Let $\mathbb{V} := \left\{x \in \mathbb{U} \,|\, x^{p-1} = 1\right\}$. Then $\mathbb{U} \cong \mathbb{V} \times \mathbb{U}_1$ canonically where $\mathbb{V}$ is isomorphic to $\mathbb{F}_p^\times$ under $\varepsilon_1^\times$ and is the unique subgroup isomorphic to $\mathbb{F}_p^\times$. Hence $\mathbb{Q}_p$ has $p-1$ roots of unity.

Proof. Consider again the short exact sequence of projective systems of abelian groups :

$$1 \to \mathbb{U}_1/\mathbb{U}_\star \to \mathbb{U}/\mathbb{U}_\star \to \underline{\mathbb{U}/\mathbb{U}_1} \to 1$$

Note that the system $\underline{\mathbb{U}/\mathbb{U}_1} \cong \underline{\mathbb{F}_p^\times}$ canonically. For $n \in \mathbb{N}$, $1 \leq n$, we have $|\mathbb{U}_1/\mathbb{U}_n| = p^{n-1}$. p^{n-1} and $p-1$ are coprime. So by coprime implies short exact, $\mathbb{V}_n = \{x \in \mathbb{U}/\mathbb{U}_n \,|\, x^{p-1} = 1\}$ has the property that $\mathbb{U}/\mathbb{U}_n \cong \mathbb{V}_n \times \mathbb{U}_1/\mathbb{U}_n$ canonically and it is the unique subgroup of $\mathbb{U}/\mathbb{U}_n$ that's isomorphic of $\mathbb{U}/\mathbb{U}_1$. Under the following commutative square

$$\begin{tikzcd}
\mathbb{U}/\mathbb{U}_{n+1} \arrow[r] \arrow[d] & \mathbb{U}/\mathbb{U}_1 \arrow[d, "1"] \\
\mathbb{U}/\mathbb{U}_n \arrow[r] & \mathbb{U}/\mathbb{U}_1
\end{tikzcd}$$

the horizontal projections map $\mathbb{V}_n, \mathbb{V}_{n+1}$ isomorphically to $\mathbb{U}/\mathbb{U}_1$. Thus $\mathbb{V}_\star$ forms a projective system of abelian groups :

$$\cdots \xrightarrow{\sim} \mathbb{V}_2 \xrightarrow{\sim} \mathbb{V}_1 \longrightarrow 1$$

With this, the first short exact sequence turns into

$$1 \to \mathbb{U}_1/\mathbb{U}_\star \to \mathbb{V}_\star \times (\mathbb{U}_1/\mathbb{U}_\star) \to \underline{\mathbb{U}/\mathbb{U}_1} \to 1$$

Finally, as noted before $\mathbb{U}_1/\mathbb{U}_\star$ is surjective, so we can pass the short exact sequence to the inverse limit.

$$1 \to \mathbb{U}_1 \to \varprojlim\,(\mathbb{V}_\star \times (\mathbb{U}_1/\mathbb{U}_\star)) \to \mathbb{U}/\mathbb{U}_1 \to 1$$

This shows that $\mathbb{U} \cong \varprojlim\,((\mathbb{U}_1/\mathbb{U}_\star) \times \mathbb{V}_\star)$ canonically. Let $\mathbb{V} := \varprojlim \mathbb{V}_\star \cong \mathbb{U}/\mathbb{U}_1$. Then since limits commute with limits, we have $\mathbb{U} \cong \mathbb{V} \times \mathbb{U}_1$ canonically. The fact that $\varepsilon_1^\times : \mathbb{V} \cong \mathbb{F}_p^\times$ comes from $\mathbb{V}_1 = \mathbb{U}/\mathbb{U}_1 \cong \mathbb{F}_p^\times$ canonically. An element $x \in \mathbb{U}$ satisfies $x^{p-1} = 1$ if and only if it satisfies it modulo p^n for all n. which is equivalent to x being in $\mathbb{V}_n$ modulo $\mathbb{U}_n$ for all n, which is in turn equivalent to $x \in \mathbb{V}$. This shows the form of $\mathbb{V}$. To show uniqueness of $\mathbb{V}$, note that any subgroup isomorphic to $\mathbb{F}_p^\times$ must satisfy $x^{p-1} = 1$ by Lagranges theorem, and hence be a subgroup of $\mathbb{V}$, and thus equal to $\mathbb{V}$.

□

Proof. Consider the polynomial $f := X^{p-1} - 1 \in \mathbb{Z}_p[X]$. The integers $x = 1, \ldots, p-1$ are roots modulo p, i.e. $\varepsilon_1(f(x)) = 0$. Furthermore, $0 = \varepsilon_1(f'(x)) = (p-1)x^{p-2} = -x^{p-2}$ implies $x = 0$, which cannot be. We thus have the conditions for Hensel's lemma, and hence have $x_1, \ldots, x_{p-1} \in \mathbb{Z}_p$ satisfying $f(x) = 0$. These elements are distinct since they are distinct modulo p. By going into $\mathbb{Q}_p$ and the factor theorem, there are at most $p-1$ elements satisfying $x^{p-1} = 1$. Hence $\mathbb{V} = \{x_1, \ldots, x_{p-1}\}$. Uniqueness of $\mathbb{V}$ follows again from Lagrange's theorem. □

Proposition – Convergence of Units to 1

Let $n \in \mathbb{N}$ such that

$$p \neq 2 \Rightarrow 1 \leq n \text{ and } p = 2 \Rightarrow 2 \leq n$$

Let $x \in \mathbb{U}_n \setminus \mathbb{U}_{n+1}$. Then $x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2}$.

Proof. We have $x = 1 + kp^n$ where $k \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Then by the binomial theorem, we have

$$x^p = 1 + kp^{n+1} + \sum_{l=2}^{p-1} \frac{(p-1)!}{l!(p-l)!} k^l p^{nl+1} + k^n p^{np}$$

For $2 \leq l$, $n+2 \leq 2n+1 \leq nl+1$. For $p = 2$, $n+2 \leq 2p$ and for $p \neq 2$, $n+2 \leq 3n \leq np$, and hence $n+2 \leq np$ in general. This shows that $\varepsilon_{n+2}(x^p) = 1 + kp^{n+1}$, which gives the desired result. □

Remark – Why Structure of $\mathbb{U}_1$ *is Not Surprising.* The following result is analogous to the fact that given any unit real α, $\mathbb{R} \cong \mathbb{R}^\times$ as abelian groups via the morphism $x \mapsto \alpha^x$.

Proposition – Structure of $\mathbb{U}_1$

The following are true :

1. Let $p \neq 2$. Then $\mathbb{U}_1 \cong \mathbb{Z}_p$ as abelian groups.
2. Let $p = 2$. Then $\mathbb{U}_1 \cong (-1)^{\mathbb{Z}} \times \mathbb{U}_2$ canonically as abelian groups where $(-1)^{\mathbb{Z}}$ is the subgroup generated by -1 and $\mathbb{U}_2 \cong \mathbb{Z}_2$ as abelian groups.

Proof. $(p \neq 2)$ Let $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, for example $1 + p$. For $n \in \mathbb{N}$, let $\alpha_n \in \mathbb{U}_1/\mathbb{U}_{n+1}$ be the image of α. Then by convergence of units to 1, we have for $k \in \mathbb{N}$, $\alpha^{p^k} \in \mathbb{U}_{1+k} \setminus \mathbb{U}_{2+k}$. So $\alpha_n^{p^n} = 1$, $\alpha_n^{p^{n-1}} \neq 1$ and $|\mathbb{U}_1/\mathbb{U}_{n+1}| = p^n$ implies $\mathbb{U}_1/\mathbb{U}_{n+1}$ is cyclic with generator α_n. From this, we can define the following morphism of projective systems :

$$\theta_\alpha : \mathbb{Z}/p^\star\mathbb{Z} \to \mathbb{U}_1/\mathbb{U}_{\star+1}$$
$$(\theta_\alpha)_n : z \in \mathbb{Z}/p^n\mathbb{Z} \mapsto \alpha_n^z \in \mathbb{U}_1/\mathbb{U}_{n+1}$$

Since α_n has order p^n, $(\theta_\alpha)_n$ is well-defined. It is clearly a morphism of abelian groups, thus θ_α is indeed a morphism of projective systems of abelian groups. We therefore have the following short exact sequence of projective systems of abelian groups :

$$0 \to 0 \to \mathbb{Z}/p^\star\mathbb{Z} \to \mathbb{U}_1/\mathbb{U}_{\star+1} \to 1$$

Since 0 is a surjective system, we can pass the isomorphism to the limit and obtain $\mathbb{Z}_p \cong \mathbb{U}_1$ as abelian groups.

$(p = 2)$ $\varepsilon_2(-1) = -1 \neq 1$ implies $\mathbb{Z}(-1) \cap \mathbb{U}_2 = \{1\}$. Since the short exact sequence

$$1 \to \mathbb{U}_2 \to \mathbb{U}_1 \xrightarrow{\varepsilon_2} (\mathbb{Z}/4\mathbb{Z})^\times \to 1$$

maps -1 to -1, $\mathbb{U}_1 = (-1)^{\mathbb{Z}}\mathbb{U}_2$. Hence $\mathbb{U}_1 \cong (-1)^{\mathbb{Z}} \times \mathbb{U}_2$ canonically as abelian groups.

For $\mathbb{U}_2 \cong \mathbb{Z}_2$, we use a similar technique to the $p \neq 2$ case. Let $\alpha \in \mathbb{U}_2 \setminus \mathbb{U}_3$, such as 5. For $n \in \mathbb{N}$, define $\alpha_n \in \mathbb{U}_2/\mathbb{U}_{n+2}$ be the image of α. Then by convergence of units to 1, we have for $k \in \mathbb{N}$, $\alpha^{p^k} \in \mathbb{U}_{2+k} \setminus \mathbb{U}_{3+k}$. So $\alpha_n^{2^n} = 1$, $\alpha_n^{2^{n-1}} \neq 1$ and $|\mathbb{U}_2/\mathbb{U}_{n+2}| = 2^n$ implies $\mathbb{U}_2/\mathbb{U}_{n+2}$ is cyclic with generator α_n. We can thus define θ_α in an analogous way to $p \neq 2$ and yield an isomorphism $\mathbb{Z}_2 \cong \mathbb{U}_2$ of abelian groups. □

Proposition – Structure of Units of $\mathbb{Q}_p$

The following are true :

- Let $p \neq 2$. Then $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{V} \times \mathbb{U}_1$ canonically as abelian groups where $p^{\mathbb{Z}}$, $(-1)^{\mathbb{Z}}$ are the subgroups generated p and -1.
- Let $p = 2$. Then $\mathbb{Q}_2^\times \cong 2^{\mathbb{Z}} \times (-1)^{\mathbb{Z}} \times \mathbb{U}_2$.

Proof. $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{U}$ from elements of $\mathbb{Q}_p^\times$ being of the form $p^n u$ where $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times = \mathbb{U}$. The rest follows from the structure of $\mathbb{U}$ and $\mathbb{U}_1$. □

Proposition – Squares in $\mathbb{Q}_p$

The following are true :

- $(p \neq 2)$ Let $x = p^n u \in \mathbb{Q}_p^\times$ where $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Then $x \in \mathbb{Q}_p^{\times(2)}$ if and only if $n \in 2\mathbb{Z}$ and $\varepsilon_1(u) \in \mathbb{F}_p^{\times(2)}$.
- $(p = 2)$ Let $x = 2^n u \in \mathbb{Q}_2^\times$ where $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_2^\times$. Then $x \in \mathbb{Q}_2^{\times(2)}$ if and only if $n \in 2\mathbb{Z}$ and $\varepsilon_3(u) = 1$.

Proof.

$(p \neq 2)$ From the structure of $\mathbb{Q}_p^\times$, we have $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{V} \times \mathbb{U}_1$. We have a decomposition of $x = p^n v u_1$ where $n \in \mathbb{Z}$, $v \in \mathbb{V}$ and $u_1 \in \mathbb{U}$. It follows that x is a square if and only if $n \in 2\mathbb{Z}$, v is a square and u_1 is a square. Since $\mathbb{U}_1 \cong \mathbb{Z}_p$ as abelian groups and scalar multiplication by 2 is surjective in $\mathbb{Z}_p$, every element of $\mathbb{U}_1$ is a square. Mapping $\varepsilon_1 : \mathbb{V} \to \mathbb{F}_p^\times$ is an isomorphism with $\varepsilon_1(v) = \varepsilon_1(u)$. So v is a square if and only if $\varepsilon_1(u)$ is a square.

$(p = 2)$ From the structure of $\mathbb{Q}_p^\times$, we have $\mathbb{Q}_2^\times \cong 2^{\mathbb{Z}} \times (-1)^{\mathbb{Z}} \times \mathbb{U}_2$. Decompose $x = 2^n (-1)^m u_2$ with $n, m \in \mathbb{Z}$ and $u_2 \in \mathbb{U}_2$. Then x is a square if and only if $n \in 2\mathbb{Z}$ and $u = u_2$ is a square. Consider the isomorphism of projective systems $\theta_\alpha : \mathbb{Z}/2^\star\mathbb{Z} \cong \mathbb{U}_2/\mathbb{U}_{2+\star}$. We have the following commutative diagram with exact rows :

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2^\star\mathbb{Z} \arrow[r, "2"] \arrow[d, "\sim"'] & \mathbb{Z}/2^\star\mathbb{Z} \arrow[d, "\sim"', "\theta_\alpha"] \\
1 \arrow[r] & \mathbb{U}_3/\mathbb{U}_{2+\star} \arrow[r] & \mathbb{U}_2/\mathbb{U}_{2+\star}
\end{tikzcd}$$

where $\mathbb{U}_3/\mathbb{U}_{2+\star}$ denotes the system

$$1 \longleftarrow \mathbb{U}_3/\mathbb{U}_3 \longleftarrow \mathbb{U}_3/\mathbb{U}_4 \longleftarrow \cdots$$

Taking inverse limits as before, we obtain an isomorphism of abelian groups $2\mathbb{Z}_2 \cong \mathbb{U}_3$ which respects the isomorphism of $\mathbb{Z}_2 \cong \mathbb{U}_2$. This shows that $\mathbb{U}_2^{(2)} = \mathbb{U}_3$. Therefore u is a square if and only if $\varepsilon_3(u) = 1$. □

Proof.

($p \neq 2$) An alternative proof for $\mathbb{U}_1 = \mathbb{U}_1^{(2)}$. Let $a \in \mathbb{U}_1$. Consider the polynomial $f := X^2 - a$. Then $\varepsilon_1(f(1)) = 0$ and $\varepsilon_1(f'(1)) = 2 \neq 0$. So by Hensel's lemma, there exists $b \in \mathbb{Z}_p$ such that $b^2 = a$ and $\varepsilon_1(b) = \varepsilon_1(1) = 1$.

($p = 2$) An alternative proof for $\mathbb{U}_2^{(2)} = \mathbb{U}_3$. The forward inclusion is given by convergence of units to 1. For the reverse inclusion, let $u \in \mathbb{U}_3$. Consider the polynomial $f := X^2 - u$. Then $\varepsilon_3(f(1)) = 0$ and $\varepsilon_2(f'(1)) = 2 - 1 = 1 \neq 0$. So by lifting solutions of quadratic forms for $p = 2$, we obtain the existence of $v \in \mathbb{Z}_2$ such that $v^2 = u$ and $\varepsilon_3(v) = \varepsilon_3(u) = 1$. This shows that $u \in \mathbb{U}_2^(2)$. $\square$

Proposition – Alternate Equivalence for being Square in $\mathbb{Q}_2$

Let $p = 2$. Define

$$\varepsilon : \mathbb{U} \to \mathbb{Z}/2\mathbb{Z}, x \mapsto \varepsilon_1\left(\frac{x-1}{2}\right) \qquad \omega : \mathbb{U}_2 \to \mathbb{Z}/2\mathbb{Z}, x \mapsto \varepsilon_1\left(\frac{x^2-1}{8}\right)$$

Then the following are true :

1. $\varepsilon : \mathbb{U}/\mathbb{U}_2 \to \mathbb{Z}/2\mathbb{Z}$ is an isomorphism of abelian groups.
2. $\omega : \mathbb{U}_2/\mathbb{U}_3 \to \mathbb{Z}/2\mathbb{Z}$ is an isomorphism of abelian groups.
3. $(\varepsilon, \omega) : \mathbb{U}/\mathbb{U}_3 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is an ismorphism of abelian groups. Hence $u \in \mathbb{U}^{(2)}$ if and only if $\varepsilon(x) = \omega(x) = 0$.

Proof.

(1) Let $x \in \mathbb{U} = 1+2\mathbb{Z}_2$. Then since $\mathbb{Z}_2$ is a integral domain, there exists a unique $\overline{x} \in \mathbb{Z}_2$ such that $x = 1+2\overline{x}$. Hence $(x-1)/2$ is well-defined. Let $y \in \mathbb{U}$, $y = 1 + 2\overline{y}$. Then

$$xy = (1+2\overline{x})(1+2\overline{y}) = 1 + 2(\overline{x} + \overline{y} + 2\overline{xy})$$

Hence $\varepsilon(xy) = \varepsilon(x) + \varepsilon(y)$. Clearly ε is surjective. It remains to show that $\ker \varepsilon = \mathbb{U}_2$. Well, $\varepsilon(x) = \varepsilon_1((x - 1)/2) = 0$ if and only if $\overline{x} \in 2\mathbb{Z}_2$ if and only if $\varepsilon_2(x) = 1$ if and only if $x \in \mathbb{U}_2$.

(2) Let $x \in \mathbb{U}_2 = 1 + 4\mathbb{Z}_2$. Then again since $\mathbb{Z}_2$ is a integral domain, there exists a unique $\overline{x} \in \mathbb{Z}_2$ such that $x = 1 + 4\overline{x}$. Then $x^2 = (1+4\overline{x})^2 = 1 + 8(\overline{x} + 2\overline{x}^2)$, hence $(x^2-1)/8$ is well-defined. Let $y = 1 + 4\overline{y} \in \mathbb{U}_2$. By similar computation as before, $\omega(xy) = \omega(x) + \omega(y)$. Clearly, ω is surjective, so it remains to show that $\ker \omega = \mathbb{U}_3$. Well, $\omega(x) = \varepsilon_1((x^2-1)/8) = 0$ if and only if $\overline{x} \in 2\mathbb{Z}_2$ if and only if $x \in \mathbb{U}_3$.

(3) By the 3rd isomorphism theorem of modules, $(\mathbb{U}/\mathbb{U}_3)/(\mathbb{U}_2/\mathbb{U}_3) \cong \mathbb{U}/\mathbb{U}_2$ canonically. Since $\mathbb{U}/\mathbb{U}_3$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}^\times$, there exists a section for the short exact sequence :

$$1 \to \mathbb{U}_2/\mathbb{U}_3 \to \mathbb{U}/\mathbb{U}_3 \to \mathbb{U}/\mathbb{U}_2 \to 1$$

Thus $\mathbb{U}/\mathbb{U}_3 \cong \mathbb{U}/\mathbb{U}_2 \times \mathbb{U}_2/\mathbb{U}_3$ and the latter is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ via (ε, ω) as claimed. The "Hence" follows from $\mathbb{U}^{(2)} = \mathbb{U}_3$, which itself follows from the structure of $\mathbb{Q}_2^\times$.

$\square$