# Notes on ...

Ken Lee, Cyclic Group 69

Date

## 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.

Conventions :

- "Rings" refer to commutative rings with unity.
- $\mathbb{N}$ denotes the naturals, including zero.

# 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 – Surjective System**

Let $R$ be a commutative ring and $F$ a projective system of $R$-modules. Then $F$ is called *surjective* when for all $n \in \mathbb{N}$, $\downarrow_n^{n+1}$ is surjective.

**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.

More explicitly, an inverse limit of $F$ is an object $A$ of $\mathcal{C}$ together with a collection of maps $(\alpha_n : A \to F_n)_{n\in\mathbb{N}}$ such that for all $n \in \mathbb{N}$, $\downarrow_n^{n+1} \alpha_{n+1} = \alpha_n$.

**Lemma – Left Surjective implies Right Exactness of Inverse Limit**

Let $R$ be a ring and

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of projective systems of $R$-modules, i.e. for all $n \in \mathbb{N}$,

$$0 \to A_n \to B_n \to C_n \to 0$$

is a short exact sequence. Then

$$0 \to \varprojlim A \to \varprojlim B \to \varprojlim C \to 0$$

is exact at $\varprojlim A$ and $\varprojlim B$. Furthermore, if $A$ is surjective, then we also have exactness at $\varprojlim C$.

**Definition – $p$-adic Integers**

Define the following projective system of 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 $n \in \mathbb{N}$, $\downarrow_n^{n+1} \varepsilon_{n+1}(x) = \varepsilon_n(x)$, where $\varepsilon_n : \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the projection into the $n$-th component.

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

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

where the middle projective system is a constant at $\mathbb{Z}$. Since taking inverse limits is left exact, we obtain the following exact sequence of $\mathbb{Z}$ modules :

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

Since the forgetful functor from the category of rings to $\mathbb{Z}$-modules is a right adjoint functor, it preserves limits. In particular, the inverse limit of $\mathbb{Z}/p^\star\mathbb{Z}$ in the category of $\mathbb{Z}$-modules is still $\mathbb{Z}_p$. It is easy to check that 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 of $\mathbb{Z}$-modules :
>
> $$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

*Proof.* (Generalized from nLab)

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

$$\begin{array}{ccccccccccc}
0 & \longleftarrow & 0 & \longleftarrow & \cdots & \longleftarrow & 0 & \longleftarrow & \mathbb{Z}/p\mathbb{Z} & \longleftarrow & \mathbb{Z}/p^2\mathbb{Z} & \longleftarrow & \cdots \\
\downarrow & & \downarrow & & & & \downarrow & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \\
0 & \longleftarrow & \mathbb{Z}/p\mathbb{Z} & \longleftarrow & \cdots & \longleftarrow & \mathbb{Z}/p^n\mathbb{Z} & \longleftarrow & \mathbb{Z}/p^{n+1}\mathbb{Z} & \longleftarrow & \mathbb{Z}/p^{n+2}\mathbb{Z} & \longleftarrow & \cdots \\
\downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longleftarrow & \mathbb{Z}/p\mathbb{Z} & \longleftarrow & \cdots & \longleftarrow & \mathbb{Z}/p^n\mathbb{Z} & \longleftarrow & \mathbb{Z}/p^n\mathbb{Z} & \longleftarrow & \mathbb{Z}/p^n\mathbb{Z} & \longleftarrow & \cdots
\end{array}$$

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

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

□

*Remark – Meaning of Truncation.* $\varepsilon_n$ 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**
> $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$.

*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 a subset of 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 $y_k := \sum_{0 \le l < k} \varepsilon_k(x^l) \in \mathbb{Z}/p^k\mathbb{Z}$ 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.

We will now give $\mathbb{Z}_p$ a norm that makes precise the intuition that higher order terms tend to zero.

> **Definition – Naturals with Infinity**
> Let $\mathbb{N}^\infty := \mathbb{N} \sqcup \{\infty\}$. Define $\le$ on $\mathbb{N}^\infty$ as follows :
>
> – For all $n, m \in \mathbb{N}^\infty \setminus \{\infty\}$, $n \le m$ is as usual.
>
> – For all $n \in \mathbb{N}^\infty$, $n \le \infty$.
>
> 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 :
>
> $$v_p : \mathbb{Z}_p \to \mathbb{N}^\infty, x \mapsto \sup \{n \in \mathbb{N}^\infty \mid \varepsilon_n(x) = 0\}$$
>
> From this, we define the *p-adic norm*,
>
> $$|\ |_p : \mathbb{Z}_p \to [0, \infty) \subseteq \mathbb{R}, x \mapsto \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0 \end{cases}$$

*Remark – Meaning of p-adic Norm.* Under the interpretation of $p$-adic integers as power series, $v_p(x)$ is the lowest power of $p$ with non-zero coefficient.

**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 – $(\mathbb{Z}_p, |\ |_p)$ 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 $|\ |_p$.

*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 $xy = p^{v_p(x)+v_p(y)}u(x)u(y)$ where $u(x), u(y) \in \mathbb{Z}_p^\times$ 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. □

> **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. □

> **Proposition – Topological Properties of $\mathbb{Z}_p$**
> The following are true :
>
> 1. (Topology) Give $\mathbb{Z}_p$ the subspace topology 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. Then for all $x \in \mathbb{Z}_p$, the set of balls $\left\{B_{p^{-n}(x)}\right\}_{n\in\mathbb{N}}$ is a prefilter that generates the neighbourhood filter of $x$ (AKA a neighbourhood base). 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 and hence a complete metric space under $|\ |_p$.
> 3. (Density of $\mathbb{Z}$ in $\mathbb{Z}_p$) For each $x \in \mathbb{Z}_p$, there exists unique $a : \mathbb{N} \to \{0, \ldots, p-1\}$ such that $x = \sum_{k=0}^{\infty} a_k p^k$. Furthermore, for all $a : \mathbb{N} \to \{0, \ldots, p-1\}$, $\sum_{k=0}^{\infty} a_k p^k$ 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 $\left\{\varepsilon_n^{-1}(\varepsilon_n(x))\right\}_{n\in\mathbb{N}} = \left\{x + p^n\mathbb{Z}_p\right\}_{n\in\mathbb{N}} = \left\{B_{p^{-n+1}}(x)\right\}_{n\in\mathbb{N}}$, 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 $a^{(k)} : \mathbb{N} \to \{0, \ldots, p-1\}$ 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 $a : \mathbb{N} \to \{0, \ldots, p-1\}, k \mapsto a^{(k)}(k)$.

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 $b : \mathbb{N} \to \{0, \dots, p-1\}$ 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 :
>
> $$|\ |_p : \mathbb{Q}_p \to [0, \infty) \subseteq \mathbb{R}, x \mapsto \begin{cases} p^{-v_p(x)} & , x \neq 0 \\ 0 & , x = 0 \end{cases}$$

> **Proposition – Topological Properties of $\mathbb{Q}_p$**
> The following are true :
>
> 1. $(\mathbb{Q}_p, |\ |_p)$ is a normed ring and hence a topological ring (field).
> 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 $|\ |_p$ 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 $\mathbb{Z}_p$. □

## 1.2 $p$-adic Equations

The goal of this section 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.

**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 $\varprojlim D$ is nonempty.

*Proof.* If $D$ is a surjective system, then $\varprojlim D$ is non-empty. We will reduce to this case.

For $n \in \mathbb{N}$, consider the descending sequence of subsets $\left\{\downarrow_n^k D_k \mid n \leq k\right\}$ 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 $\varnothing \neq \varprojlim E \to \varprojlim D$. □

*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 $I \subseteq \mathbb{Z}_p[X_1, \ldots, X_m]$, let $I_n$ denote the image of $I$. For a single polynomial $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, let $f_n$ denote its image. More explicitly, for $f = \sum_{t \in \mathbb{N}^m} a_t \underline{X}^t$,

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

**Definition – Vanishing**
Let $A$ be a ring, $m \in \mathbb{N}$, $I \subseteq A[X_1, \ldots, X_m]$. Then $\mathbb{V}_A(I) \subseteq A^m$ is defined as the tuples $x$ such that for all $f \in I$, $f(x) = 0$. When the ring in question is clear, we abbreviate to $\mathbb{V}(I)$.

**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 $\mathbb{V}(I) \cong \varprojlim \mathbb{V}(I_\star)$ 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.* First note that since limits commute with limits, $\mathbb{Z}_p^m \cong \varprojlim (\mathbb{Z}/p^\star\mathbb{Z})^m$.

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 $n \in \mathbb{N}$, let $\varepsilon_n^m : \mathbb{Z}_p^m \to \mathbb{Z}/p^n\mathbb{Z}^m$ denote the natural projection. Then

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

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 $\mathbb{V}(I) \cong \varprojlim \mathbb{V}(I_\star)$ under the isomorphism $\mathbb{Z}_p^m \cong \varprojlim (\mathbb{Z}/p^\star\mathbb{Z})^m$.

The 'in particular' follows from inverse limit of finite, nonempty is nonempty. □

**Definition – Primitive Solutions**

Let $m, n \in \mathbb{N}^+$. Let $\varepsilon_1^m : \mathbb{Z}_p^m \to \mathbb{Z}/p\mathbb{Z}^m$ and $(\downarrow_1^n)^m : \mathbb{Z}/p^n\mathbb{Z}^m \to \mathbb{Z}/p\mathbb{Z}^m$ be the natural projections. 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 $h := \inf \{v_p(x_i) \,|\, i = 1, \ldots, m\}$. 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, $\varprojlim P$ injects into $\mathbb{V}_{\mathbb{Z}_p}(I)$ canonically. We identify it with its image. Clearly, for any $x \in \varprojlim P$, $\varepsilon_1(x) \neq 0$. So $\varprojlim P$ 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 $\varprojlim P$ that maps to $x$. Hence $\varprojlim P$ is equal to the set of primitives in $\mathbb{V}_{\mathbb{Z}_p}(I)$. □

**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. □

**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 $\leq 1$, 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 $|\ |_p$, 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 :

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

The implication followed from $|\mathbb{Z}_p|_p = \{1, p^{-1}, p^{-2}, \ldots, 0\}$. It remains to show $|f'(\overline{x})|_p = |f'(x)|_p$. By applying mean value theorem to $f'$, we have for some $d, e \in \mathbb{Z}_p$,

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

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 $|f'(\overline{x})|_p = \left||f'(x)|_p^{-1}\right|_p = |f'(x)|_p$. □

> **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
>
> $$|f(x)|_p < \left|\frac{\partial f}{\partial X_j}\right|_x\Bigg|_p^2$$
>
> Then there exists $y \in \mathbb{Z}_p^m$ such that $f(y) = 0$ and
>
> $$\max(|\pi_i(y - x)|_p)_{1 \leq i \leq m} \leq \frac{|f(x)|_p}{\left|\frac{\partial f}{\partial X_j}\right|_x\Big|_p}$$
>
> 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

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

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 $k \in \mathbb{N}$,

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

We see that $\lim_{k\to\infty} f(x_k) = 0$. Furthermore, from the ultrametric property of $|\ |_p$, 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 $|\ |_p$, the fact that $\mathbb{Z}_p \to \mathbb{Z}_p, x \mapsto f(x)$ is defined by finitely many additions and multiplications implies 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 and induction on $k$, we have

$$|x_{k+1} - x|_p \leq \max\left(|x_{k+1} - x_k|_p, |x_k - x|_p\right) \leq \max\left(\frac{|f(x_0)|_p}{p^k |f'(x_0)|_p}, \frac{|f(x_0)|_p}{|f'(x_0)|_p}\right) \leq \frac{|f(x_0)|_p}{|f'(x_0)|_p}$$

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

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

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 :

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

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

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

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 $f$, evaluating at $x$ and reducing mod 4, we have

$$\left[\varepsilon_2\left(\frac{\partial f}{\partial X_i}\bigg|_x\right)\right]_{i=1}^m = 2[\varepsilon_2(a_{ij})]_{i,j=1}^m \varepsilon_2(x)$$

Since $\det[a_{ij}]_{i,j=1}^m \in \mathbb{Z}_2^\times$, $\det[\varepsilon_2(a_{ij})]_{i,j=1}^m \in \mathbb{Z}/2^2\mathbb{Z}^\times$, the fact that $\varepsilon_2(x)$ is not a multiple of 2 implies the tuple $[\varepsilon_2(a_{ij})]_{i,j=1}^m \varepsilon_2(x)$ is not a multiple of 2. The existence of $i$ such that $\varepsilon_2\left(\frac{\partial f}{\partial X_i}\Big|_x\right) \neq 0$ follows. □

## 1.3 Appendix : Omitted Proofs

*Proof.* (Left Surjective implies Right Exactness of Inverse Limit - from Atiyah)

It is elementary to check that we have the short exact sequence of $R$-modules

$$0 \to \prod A \to \prod B \to \prod C \to 0$$

where $\prod$ takes the product of $R$-modules. For $n \in \mathbb{N}$, let $\pi_n : \prod A \to A_n$ be the natural projection. Note that we have a canonical map

$$\varprojlim A \xrightarrow{\prod \varepsilon} \prod A$$

induced from the natural maps $\varepsilon_n : \varprojlim A \to A_n$ for $n \in \mathbb{N}$. Define $d^A : \prod A \to \prod A$ via $d_n^A : \prod A \to A_n :=\downarrow_n^{n+1} \pi_{n+1} - \pi_n$ and the universal property of $\prod A$. Define $d^B, d^C$ similarly for $B, C$ and we have the following commutative diagram of $R$-modules with exact rows :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod A & \longrightarrow & \prod B & \longrightarrow & \prod C & \longrightarrow & 0 \\ & & \downarrow d^A & & \downarrow d^B & & \downarrow d^C & & \\ 0 & \longrightarrow & \prod A & \longrightarrow & \prod B & \longrightarrow & \prod C & \longrightarrow & 0 \end{array}$$

Applying the snake lemma, we obtain exact sequence of $R$-modules :

$$0 \longrightarrow \ker d^A \longrightarrow \ker d^B \longrightarrow \ker d^C \longrightarrow \operatorname{coker} d^A \longrightarrow \operatorname{coker} d^B \longrightarrow \operatorname{coker} d^C \longrightarrow 0$$

It is straight forward to check that $\varprojlim A, \varprojlim B, \varprojlim C$ are respectively the kernels of $d^A, d^B, d^C$ and that $A$ surjective implies the zero module 0 is the cokernel of $d^A$. The result follows. □

*Proof.* (Truncation - from Serre)

(*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*) $\varepsilon_n$ 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 $0 \leq x_{n+k} < p^{n+k}$, there exists a unique $0 \leq y_k < p^k$ 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, $x = p^n y \in p^n\mathbb{Z}_p$. □

*Proof.* ($\mathbb{Z}_p$ Local Ring - from Serre)

We first prove that for $n \geq 1$, $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with maximal ideal $p\mathbb{Z}/p^n\mathbb{Z}$. 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. $x \in \mathbb{Z}_p^\times$. □

# References