Number Theory Notes

JH

Date

Contents

Chapter 1

Finite Fields

1.1 Generalities

1.1.1 Finite fields

Definition – Characteristic of a field
If K is a field then the map $\mathbb{Z} \to K$ induced by $1 \mapsto 1$ is a ring morphism. The image of this morphism is an integral domain since K is a field, hence the kernel is a prime ideal. Since $\mathbb{Z}$ is a PID, we can define the characteristic of K, denoted $\mathrm{Char}(K)$ to be the positive generator of the kernel. [a]

[a] A foot

Proposition – Frobenius map
If K is a field and $\mathrm{Char}(K)$ is prime then

$$\sigma_p : K \to K \quad := \quad x \mapsto x^p$$

is an injection.

Proof. Easy to show $\sigma_p(0) = 0, \Sigma_p(1) = 1$. Also

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\sigma_p(b)$$

$$\sigma_p(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

by expanding the binomial and noting that when $1 \leq k \leq p$, $p \mid \binom{p}{k} k!(p-k)!$ and is coprime to the latter two, thus $p \mid \binom{p}{k}$. Since σ_p is a morphism of fields it is injective. □

Proposition – Classification of finite fields

Let K be a finite field and suppose $\Omega \models \mathrm{ACF_p}$ where p is prime and q is a non-trivial power of p. Then

1. $\mathrm{Char}(K) \neq 0$ and $|K| = p^{[K:\mathbb{F}_p]}$
2. $\mathbb{F}_q := \{x \in \Omega \mid x^q = x\}$ is the unique subfield of Ω with q elements.
3. If $|K| = q$ then $K \cong \mathbb{F}_q$.

Proof.

1. If $\mathrm{Char}(K) = 0$ then $\mathbb{Z}$ injects into K thus thus $\aleph_0 \leq |\mathbb{Z}| \leq |K|$ which is false. Since $[K : \mathbb{F}_p]$ is the cardinality of any basis B of K as a vector space over $\mathbb{F}_p$ and $K \cong {\mathbb{F}_p}^B$, $|K| = \left|{\mathbb{F}_p}^B\right| = p^{[K:\mathbb{F}_p]}$.
2. Easy to show elementarily that $\mathbb{F}_q$ is a subfield. As polynomials over a field are seperable if and only the gcd of the derivative and the polynomial is 1,
$$D(X^q - X) = qX^{q-1} - 1 = -1$$
Hence it has q distinct roots in the algebraic closure of Ω, namely Ω itself. Hence $|\mathbb{F}_q| = q$. Uniqueness: if $L \leq \Omega$ and $|L| = q$ then for any unit $x \in L \setminus \{0\}$, $x^{q-1} = 1$ by Lagrange and so $x \in \mathbb{F}_q$. Thus $L \subseteq \mathbb{F}_q$ and they have equal finite cardinality, so $L = \mathbb{F}_q$.
3. If L is a field such that $|L| = q$ then the image of $\mathbb{Z}$ in L has cardinality dividing q by Lagrange. Hence $\mathrm{Char}(L) = p$ and the image of $\mathbb{Z}$ is $\mathbb{F}_p$. Finitely generate L over $\mathbb{F}_p$ and for each generator a the minimal polynomial of a over $\mathbb{F}_p$ splits in Ω since it is aglebraically closed. By 'embedding finite extensions via conjugates' in Galois Theory, there is a map $L \to F_q$ which is injective. It is an isomorphism since they have the same finite cardinality.

□

1.1.2 Multiplicative group of a finite field

Definition – Euler's Totient Function

If $1 \leq a \leq d$ in $\mathbb{Z}$ then a is coprime to d if and only if $\overline{a} \in \mathbb{Z}/d\mathbb{Z}$ is a generator since

$$\begin{aligned} & (a,d) = 1 \\ \Leftrightarrow\ & \exists \lambda, \mu \in \mathbb{Z}, \lambda a + \mu d = 1 \\ \Leftrightarrow\ & \exists \lambda \in \mathbb{Z}, \overline{\lambda a} = 1 \\ \Leftrightarrow\ & \langle \overline{a} \rangle = \mathbb{Z}/d\mathbb{Z} \end{aligned}$$

We define Euler's totient function

$$\phi(d) := |\{a \in \mathbb{Z}/d\mathbb{Z} \mid \langle a \rangle = \mathbb{Z}/d\mathbb{Z}\}| = |\{a \in \mathbb{Z} \mid 1 \leq a \leq d \wedge (a,d) = 1\}|$$

Notation. *For any cyclic group G, let $\Phi(G) = \{g \in G \mid \langle g \rangle = G\}$ be the set of generators.*

Proposition – Partitioning cyclic groups
If $n \in \mathbb{Z}_{>0}$ then $n = \sum_{d|n} \phi(d)$.

Proof. Let $n \in \mathbb{Z}_{>0}$ and let d divide n. Then by some cyclic group theory there exists a unique cyclic subgroup $C_d \leq \mathbb{Z}/n\mathbb{Z}$ with cardinality d. We want to show that $\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \Phi(C_d)$. Indeed if $x \in \mathbb{Z}/n\mathbb{Z}$ then $\langle x \rangle$ has some order d dividing n by Lagrange. Hence $x \in \Phi(\langle x \rangle) = \Phi(C_d)$. Thus $\mathbb{Z}/n\mathbb{Z} \subseteq \cup_{d|n} \Phi(C_d)$.

To show it is disjoint notice that if x is in $\Phi(C_d) \cap \Phi(C_e)$ then d and e are both the order of x. □

Proposition – Sufficient condition for cyclic
Let G be a group such that for any $d \mid |G|$,

$$\left|\left\{x \in G \,|\, x^d = e\right\}\right| \leq d$$

then G is cyclic.

Proof. We show that for all divisors of $|G|$ there is an element of G of that order. Then in particular $|G| \mid |G|$ and so there is a generator of G.

Let $d \mid G$. Consider $\{x \in G \,|\, x \text{ has order } d\}$. If it is non-empty, then take such an x:

$$\langle x \rangle \subseteq \left\{g \in G \,|\, g^d = e\right\}$$

and so $d \leq |\langle x \rangle| \leq \left|\left\{g \in G \,|\, g^d = e\right\}\right| \leq d$. Then $\langle x \rangle = \left\{g \in G \,|\, g^d = e\right\}$. Hence for $g \in G$,

$$\begin{aligned} g \text{ has order } d &\Leftrightarrow g \text{ has order } d \wedge g^d = e \\ &\Leftrightarrow g \text{ has order } d \wedge g \in \langle x \rangle \\ &\Leftrightarrow \langle g \rangle = \langle x \rangle \end{aligned}$$

Hence $|\{x \in G \,|\, x \text{ has order } d\}| = \phi(d)$ In either case, (empty or not), $|\{x \in G \,|\, x \text{ has order } d\}| \leq \phi(d)$

Assume for a contradiction that there exists a d such that $\{x \in G \,|\, x \text{ has order } d\}$ is empty. Then partitioning

$$G = \bigsqcup_{d \,\mid\, |G|} \{x \in G \,|\, x \text{ has order } d\}$$

we have that

$$|G| = \sum_{d||G|} |\{x \in G \,|\, x \text{ has order } d\}| < \sum_{d||G|} \phi(d) = |G|$$

a contradiction. □

Proposition – $\mathbb{F}_q^*$ is cyclic
Suppose $d \mid \left|\mathbb{F}_q^*\right|$. Then since $\mathbb{F}_q[X]$ has division algorithm,

$$\left|\left\{x \in \mathbb{F}_q^* \,|\, x^d = 1\right\}\right| \leq d$$

Hence $\mathbb{F}_q^*$ is cyclic.

1.2 Equations over a finite field

Proposition

Power sums lemma Let $u \in \mathbb{N}$ and K be field with $|K| = q$ a power of a non-trivial prime. Then

$$\sum_{x \in K} x^u = \begin{cases} -1 & , 1 \leq u \wedge q-1 \mid u \\ 0 & , \text{otherwise} \end{cases}$$

Proof. Case $u = 0$ then $\sum_{x \in K^n} x^u = \sum_{x \in K^n} 0 = 0$.

Case $1 \leq u \wedge q-1 \mid u$ then for some d,

$$\sum_{x \in K} x^u = \sum_{x \in K} (x^(q-1))^d == \sum_{x \in K^*} 1^d = (q-1)1 = -1$$

Case $1 \leq u \wedge q-1 \nmid u$ then there exist $d, r \in \mathbb{N}$ such that $u = (q-1)d + r$ and $0 < r < q-1$. Let y be a generator of K^* (K^* is cyclic). Then suppose for a contradiction that $y^u = 1$, then $q-1 \mid u$ since $q-1$ is the order of y, a contradiction. Multiplying by y is a bijection on the group, hence

$$\sum_{x \in K^n} x^u = \sum_{x \in K^n} (yx)^u = y^u \sum_{x \in K^n} x^u$$

Thus $(1 - y^u) \sum_{x \in K^n} x^u = 0$ and so $\sum_{x \in K^n} x^u = 0$, as $y^u \neq 1$. □

Definition – Vanishing

Let R be a ring. Suppose for all $I \subseteq R[x1, \ldots, x_n]$ We define the vanishing of I in R,

$$\mathbb{V}(I, R) := \{x \in R^n \mid \forall f \in I, f(x) = 0\}$$

If the context is obvious we just write $\mathbb{V}(I)$.

Proposition – Chevalley

Suppose for all $f \in I \subseteq K[x_1, \ldots, x_n]$ (finite),

$$\sum_{f \in I} \deg f < n$$

Then

$$|\mathbb{V}(I)| \stackrel{p}{=} 0$$

Proof. Consider $P := \prod_{f\in I}(1 - f^{q-1})$. This is well defined as I is finite. We show that $\mathbb{V}(I) = P^{-1}(1)$. Let $x \in K^n$.

$$x \in \mathbb{V}(I) \Rightarrow \forall f \in I, f(x) = 0 \Rightarrow f(x)^{q-1} = 0 \Rightarrow P(x) = 1$$

$$x \notin \mathbb{V} \Rightarrow \exists f \in I, f \neq 0 \Rightarrow f(x)^{q-1} = 1 \Rightarrow P(x) = 0$$

Let $S : K[x_1, \dots, x_n] \to K := f \to \sum_{x\in K^n} f(x)$ Then $S(P) = \sum_{x\in V(I)} 1 \overset{p}{=} |\mathbb{V}(I)|$. Thus we need show that $S(P) = 0$.

$$\deg P = \sum_{f\in I}(q-1)\deg f = (q-1)\sum_{f\in I}\deg f < n \Rightarrow < (q-1)n$$

by assumption. Hence there exists a finite set T and $\lambda_i \in K$ such that

$$P = \sum_{i\in T}\lambda_i \prod_{j=1}^{n} x_j^{u_{ij}}$$

and for all $i \in T$, $\sum_{j=1}^{n} u_{ij} < (q-1)n$. Then

$$\begin{align} S(P) &= \sum_{x\in K^n} P(x) \tag{1.1}\\ &= \sum_{x\in K^n}\sum_{i\in T}\lambda_i \prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.2}\\ &= \sum_{i\in T}\lambda_i \sum_{x\in K^n}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.3}\\ & \tag{1.4}\end{align}$$

Let $i \in T$ then there exists a k such that $u_{ik} < q-1$ so

$$\begin{align} &\sum_{x\in K^n}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.5}\\ =&\sum_{x_1\in K}\cdots\sum_{x_n\in K}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.6}\\ =&\sum_{x_1\in K}\cdots\cancel{\sum_{x_k\in K}}\cdots\sum_{x_n\in K}\prod_{j\neq k} x_j^{u_{ij}}\sum_{x_k\in K} x_k^{u_{ik}} \tag{1.7}\\ =&\sum_{x_1\in K}\cdots\cancel{\sum_{x_k\in K}}\cdots\sum_{x_n\in K}\prod_{j\neq k} x_j^{u_{ij}}0 \tag{1.8}\end{align}$$

The last part using the power sum lemma. Hence $|\mathbb{V}(I)| \overset{p}{=} S(P) = 0$ $\square$

Corollary – Non-trivial vanishing
Suppose for all $f \in I \subseteq K[x_1, \ldots, x_n]$ (finite),

$$\sum_{f \in I} \deg f < n$$

and $0 \in \mathbb{V}(I)$ then $\exists x \in \mathbb{V}(I) \setminus \{0\}$.

Proof. If $|V| = 1$ then $p \not| |\mathbb{V}|$ which is a contradiction. Thus the vanishing is non-trivial. □

Definition – Homogeneous
$f \in K[x_1, \ldots, x_n]$ is homogeneous with degree m if all monomials are of degree m.

Corollary – Conics over a finite field
If $3 \leq n$ then if $f \in K[x_1, \ldots, x_n]$ is homogeneous with degree 2 then it has a non-trivial zero.

1.3 Quadratic reciprocity

Proposition – Exact sequence
If K is a finite field,

- If $\mathrm{Char}(K) = 2$ then all elements are square.
- If $\mathrm{Char}(K) \neq 2$ then the non-zero squares form a subgroup of index 2, and is the kernel of the group morphism $x \to x^{\frac{q-1}{2}}$ into $\langle -1 \rangle$.

I can't be bothered to make the exact sequence.

Proof.

- If $\mathrm{Char}(K) = 2$ then the Frobenius map $\sigma_2 : x \mapsto x^2$ is an automorphism of K. Hence the preimage of any element squares to that element.
- If $\mathrm{Char}(K) \neq 2$ then generate $K^* = \langle g \rangle$ since it is cyclic. The map $x \to x^{\frac{q-1}{2}}$ has kernel $\{x \in K \mid x \text{ square}\}$ since (writing any element as a multiple of g)

  $$g^n \in \ker \Leftrightarrow g^{\frac{n(q-1)}{2}} = 1 \Leftrightarrow q - 1 \mid \frac{n(q-1)}{2} \Leftrightarrow n \text{ even} \Leftrightarrow x \text{ square}$$

  We check where the generator g is sent. If $g^{\frac{q-1}{2}} = 1$ then the order of g is less than $q - 1$ which is a contradiction hence the image is non-trivial. Any element of the image of the map squares to 1 hence solves $x^2 - 1 = 0$, which only has two solutions in K. Thus the image is $\langle -1 \rangle$ and the index of the kernel is 2.

□

Definition – Legendre symbol
If p is prime that is not 2 and $x \in \mathbb{F}_p$ then

$$\left(\frac{x}{p}\right) := \begin{cases} x^{\frac{p-1}{2}} & , x \text{ unit} \\ 0 & , x = 0 \end{cases}$$

Check that for each p this is a homomorphism $\mathbb{F}_p \to \langle -1 \rangle$.

Definition – $\varepsilon(n)$
If $n \in \mathbb{Z}$ is odd

$$\varepsilon(n) := \frac{n-1}{2} (\text{mod} 2)$$

Proposition – Computations

$$\left(\frac{1}{p}\right) = 1$$
$$\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$$

Proposition – Quadratic reciprocity
Let $l \neq p$ be primes that aren't 2. Then

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}$$

Proof. Let w be order l element of Ω, the algebraic closure of $\mathbb{F}_p$. For $x \in \mathbb{F}_l$ write w^x to be w^r for any $r \in \mathbb{Z}$ such that $x = \overline{r} \in \mathbb{F}_l$ (independant of choice of r by $w^l = 1$). Let

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x \in \Omega$$

We first show that $y^2 = (-1)^{\varepsilon(l)}\bar{l}$, where $\bar{l} \in \mathbb{F}_p$.

$$\begin{aligned}
y^2 =& (\sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right) w^x)(\sum_{y\in\mathbb{F}_l} \left(\frac{y}{l}\right) w^y) \\
=& \sum_{x\in\mathbb{F}_l}\sum_{y\in\mathbb{F}_l} \left(\frac{x}{l}\right) w^x \left(\frac{y}{l}\right) w^y \\
=& \sum_{x\in\mathbb{F}_l}\sum_{y\in\mathbb{F}_l} \left(\frac{xy}{l}\right) w^{x+y} \\
=& \sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l} \left(\frac{x(u-x)}{l}\right) w^u
\end{aligned}$$

Case on what x is:

$$\begin{aligned}
x \neq 0 \Rightarrow \left(\frac{x(u-x)}{l}\right) =& \left(\frac{xu-x^2}{l}\right) \\
=& \left(\frac{x^2}{l}\right)\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right) \\
=& x^{p-1}\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right) \\
=& (-1)^{\varepsilon(l)}\left(\frac{1-\frac{u}{x}}{l}\right)
\end{aligned}$$

If $x = 0$ then clearly $\left(\frac{x(u-x)}{l}\right) = 0$. Hence

$$y^2 = \sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*} (-1)^{\varepsilon(l)}\left(\frac{1-\frac{u}{x}}{l}\right) = (-1)^{\varepsilon(l)}\sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right)$$

Given $x \neq 0$, case on what u is:

$$\begin{aligned}
u = 0 \Rightarrow& \sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right) \\
=& \sum_{x\in\mathbb{F}_l^*}\left(\frac{1}{l}\right) \\
=& \sum_{x\in\mathbb{F}_l^*} 1 \\
=& \bar{l} - 1
\end{aligned}$$

$$\begin{aligned}
u \neq 0 \Rightarrow \sum_{x \in \mathbb{F}_l^*} \left(\frac{1 - \frac{u}{x}}{l} \right) \\
&= \sum_{x \in F_l^*} \left(\frac{1 - \frac{1}{x}}{l} \right) \\
&= \sum_{s \in \mathbb{F}_l^*} \left(\frac{1 - s}{l} \right) \\
&= \sum_{s \in \mathbb{F}_l \setminus \{1\}} \left(\frac{s}{l} \right) \\
&= \sum_{s \in \mathbb{F}_l} \left(\frac{s}{l} \right) - \left(\frac{1}{l} \right) \\
&= -1
\end{aligned}$$

Since the index of the kernel of $\left(\frac{*}{l}\right)$ is 2, and the cosets have equal cardinality. Hence

$$\begin{aligned}
y^2(-1)^{\varepsilon(l)} &= \sum_{u \in \mathbb{F}_l} \sum_{x \in \mathbb{F}_l^*} \left(\frac{1 - \frac{u}{x}}{l} \right) \\
&= \bar{l} - 1 - \sum_{u \in \mathbb{F}_l^*} w^u \\
&= \bar{l} - (1 + w + w^2 + \cdots + w^l)
\end{aligned}$$

since l is prime. Note that $0 = w^l - 1 = (w+1)(1+w+\cdots+w^l)$. Hence $1+w+\cdots+w^l = 0$ and $y^2 = (-1)^{\varepsilon(l)}\bar{l}$.

Next we show that $y^{p-1} = \left(\frac{p^{-1}}{l}\right)$.

$$\begin{aligned}
y^p &= \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l} \right)^p w^x p && \text{'Freshman's dream'} \\
&= \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l} \right) w^x p && \left(\frac{x}{l} \right) = \pm 1 \text{ and } p \text{ is odd} \\
&= \sum_{z \in \mathbb{F}_l} \left(\frac{zp^{-1}}{l} \right) w^z \\
&= \left(\frac{p^{-1}}{l} \right) (\sum_{z \in \mathbb{F}_l} \left(\frac{z}{l} \right) w^z) \\
&= \left(\frac{p^{-1}}{l} \right) y
\end{aligned}$$

Hence

$$y^{p-1} = \left(\frac{p^{-1}}{l} \right) = (\left(\frac{pl}{)} \right)^{-1}$$

thus

$$\begin{aligned}
\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) &= \left(\frac{l}{p}\right) y^{1-p} \\
&= \left(\frac{l}{p}\right) (y^2)^{\frac{1-p}{2}} \\
&= \left(\frac{l}{p}\right) ((-1)^{\varepsilon(l)}\bar{l})^{\frac{1-p}{2}} \\
&= \left(\frac{l}{p}\right) (\left(\frac{(-1)^{\varepsilon(l)}l}{p}\right))^{-1} \\
&=(\left(\frac{(-1)^{\varepsilon(l)}}{p}\right))^{-1} \\
&=(-1)^{\varepsilon(l)\varepsilon(p)}
\end{aligned}$$

□

Chapter 2

p-adic Fields

2.1 p-adic Integers and Rationals

Definition – Projective system
Let $\mathcal{C}$ be a category. A contravariant functor $F : (\mathbb{N}, \leq) \to \mathcal{C}$ is called a projective system.

Definition – Projective system A
Define a contravariant functor $A : (\mathbb{N}, \leq) \to$ **Ring** such that for each n

$$A_n := \mathbb{Z}/p^n\mathbb{Z} \quad \text{and} \quad \pi_n : \mathbb{Z} \to A_n \text{ is the projection}$$

and for any n such that $1 \leq n$, there exists a surjective ring morphism $\phi_n : A_n \to A_{n-1}$ such that $\phi_n \circ \pi_n = \pi_{n-1}$ and $\ker(\phi_n) = p^{n-1}A_n$.

Exercise. *Check that such a ϕ_n exists.*

Definition – p-adic integers
Let

$$\mathbb{Z}_p = \{x \in \prod_{n\in\mathbb{N}} A_n \mid (\forall n \in \mathbb{N}, x_n \in A_n) \wedge (\forall n > 0, \phi_n(x_n) = x_{n-1})\}$$

be the projective limit. Define addition and multiplication pointwise. Verify that this $\mathbb{Z}_p$ is a ring with $0 = (0)_{n\in\mathbb{N}}$ and $1 = (1)_{n\in\mathbb{N}}$.

For each $n \in \mathbb{N}$ let $\varepsilon_n : \mathbb{Z}_p \to A_n$ be the ring morphisms mapping $x \mapsto x_n$. Note that by definition $\phi_n \circ \varepsilon_n = \varepsilon_{n-1}$.

In addition, provide each A_n with the discrete toplogy, giving $\prod_{n\in\mathbb{N}} A_n$ the product topology and $\mathbb{Z}_n$

the subset topology.

Proposition – $\mathbb{Z}_p$ is compact
Since each A_n is finite, each A_n is compact. Hence by Tychonoff's theorem the product is compact. Since closed in compact is compact we just need to show that $\mathbb{Z}_p$ is closed.

We want to write $\mathbb{Z}_p$ as the intersection of closed sets

$$D_k := \left\{ x \in \prod_{n \in \mathbb{N}} A_n \mid \phi_k(x_k) = x_{k-1} \right\}$$

for $k \in \mathbb{N}$. Clearly

$$\bigcap_{k \in \mathbb{N}} D_k = \mathbb{Z}_p$$

and

$$D_k = \bigcup_{x_{k-1} \in A_{k-1}} \left(\varepsilon_{k-1}^{-1}(x_{k-1}) \cap \bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\} \right)$$

Since each $\{x_k\}$ is closed in A_k, each preimage $\varepsilon_k^{-1}(x_k)$ is closed. Thus the finite union of the preimages

$$\bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\}$$

is closed. Since each $\{x_{k-1}\}$ is closed in A_{k-1}, each preimage $\varepsilon_{k-1}^{-1}(x_{k-1})$ is closed. Thus intersection

$$\left(\varepsilon_{k-1}^{-1}(x_{k-1}) \cap \bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\} \right)$$

is closed. Hence the finite union is closed and D_k is closed. Arbitrary intersection of closed is closed so $\mathbb{Z}_p$ is closed and thus compact.

Proposition – Universal property of $\mathbb{Z}_p$
Suppose R is a ring with ring morphisms $\rho_n : R \to A_n$ for each $n \in \mathbb{N}$ such that for each $n > 0$, $\phi_n \circ \rho_n = \rho_{n-1}$. Then there exists a unique ring morphism $f : R \to \mathbb{Z}_p$ such that for each n, $\varepsilon_n \circ f = \rho_n$.

Proof. If there exists such a map then it is unique: suppose f, g both satisfy the given properties. Then for any n and any $a \in R$ $\varepsilon_n \circ f(a) = \rho_n(a) = \varepsilon_n \circ g(a)$. Thus $f(a) = g(a)$, by the property of products (if they agree on all the projections they are equal).

For existence we let $a \in R$ and consider the set

$$\bigcap_{n \in \mathbb{N}} \varepsilon_n^{-1} \circ \rho_n(a)$$

show that it has cardinality 1, and let f map a to this unique element. If $x, y \in \bigcap_{n \in \mathbb{N}} \varepsilon_n^{-1} \circ \rho_n(a)$ then for any $n \in \mathbb{N}$, $\varepsilon_n(x) = \rho_n(a) = \varepsilon_n(y)$. Thus $a = b$ by the property of products. Hence the cardinality is ≤ 1.

To show that the set is non-empty, take $x = (\rho_n(a))_{n\in\mathbb{N}}$. This is in $\mathbb{Z}_p$ since for each $n > 0$, $\phi_n \circ \rho_n(a) = \rho_{n-1}(a)$. Also it is in the intersection since for each n, $\varepsilon_n(x) = \rho_n(a)$. Hence the cardinality is 1. Hence f is well-defined and for all $n \in \mathbb{N}$, $\varepsilon_n \circ f = \rho_n$.

For any n,

$$\varepsilon_n \circ f(a+b) = \rho_n(a+b) = \rho_n(a) + \rho_n(b) = \varepsilon_n \circ f(a) + \varepsilon_n \circ f(b) = \varepsilon_n(f(a) + f(b))$$

Hence by property of products $f(a+b) = f(a) + f(b)$ and similarly for multiplication. Note that for any n, $\varepsilon_n \circ f(1) = \rho_n(1) = 1$. Hence $f(1) = 1$. Thus f is a ring morphism. ☐

> **Corollary – $\mathbb{Z}$ injects into $\mathbb{Z}_p$**
> Then there exists a unique injective ring morphism $\iota : \mathbb{Z} \to \mathbb{Z}_p$ such that for each n, $\varepsilon_n \circ \iota = \pi_n$.

Proof. By the previous theorem the morphism exists and is unique. It must send $1 \mapsto 1$ hence $\iota(x) = 0$ would imply $\pi_n(x) = \varepsilon_n \circ \iota(x) = 0$ for all $n \in \mathbb{N}$. Hence for any $n \in \mathbb{N}$, $p^n \mid x$. Thus $x = 0$. ☐

> **Proposition – Multiplying by p^n is injective and $x_n = 0$ implies $x \in p^n\mathbb{Z}_p$**
> $$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n \cdot} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \longrightarrow 0$$
> is a short exact sequence of abelian groups.

Proof. To check that the morphism $\mathbb{Z}_p \to \mathbb{Z}_p$ multiplying by p^n is injective it suffices to show that multiplying by p is injective. Suppose x is in the kernel of this map, then $px = 0$ thus for any n, $px_{n+1} = \varepsilon_{n+1}(px) = 0$. We show that for any n, $x_n = 0$. There exists $a \in \mathbb{Z}$ such that $\pi_{n+1}(a) = x_{n+1}$. Since $\pi_{n+1}(pa) = px_{n+1} = 0$, $pa = p^{n+1}b$ for some $b \in \mathbb{Z}$. Hence $a = p^n b$ since $\mathbb{Z}$ is an integral domain. Thus $\pi_n(a) = x_n = 0$. Thus $x = 0$.

To check that the $p^n\mathbb{Z}_p = \ker(\varepsilon_n)$ we note that for any $x \in \mathbb{Z}_p$, $\varepsilon_n(p^n x) = p^n x_n = 0 \in A_n$. Hence $p^n\mathbb{Z}_p \subseteq \ker(\varepsilon_n)$. For the other direction suppose $\varepsilon_n(x) = 0$. Suppose $n \le m \in \mathbb{Z}$. Then there exists a unique $a_m \in \mathbb{Z}$ such that $0 \le a < p^m$ and $\pi_m(a_m) = \varepsilon_m(x)$. Then

$$\pi_n(a_m) = \phi_m \circ \cdots \circ \phi_{n+1}\pi_m(a_m) = \phi_m \circ \cdots \circ \phi_{n+1}\varepsilon_m(x) = \varepsilon_n(x) = 0$$

Thus there exists a unique $b_m \in \mathbb{Z}$ such that $a_m = p^n b_m$.

Let $b = (\pi_m(b_m))_{m\in\mathbb{N}} \in \mathbb{Z}_p$. Note that multiplying by p^n commutes with all the map as they are ring homomorphisms. Then for any $m \in \mathbb{N}$,

$$\begin{aligned} \phi_{m+1}\varepsilon_{m+1}(b) &= \phi m + 1 \circ \pi_{m+1}(b_{m+1}) & &= \phi m + 1 \circ \pi_{m+1}(p^n a_{m+1}) \\ &= p^n \phi_{m+1} \circ \pi_{m+1}(p^n a_{m+1}) & &= p^n \pi_m(a_m) \\ &= \pi_m(b_m) & &= \varepsilon_m(b) \end{aligned}$$

Hence $b \in \mathbb{Z}_p$. Furthermore, let $m \in \mathbb{N}$ then

$$\varepsilon_m(p^n b) = p^n \pi_m(b_m) = \pi_m(p^n b_m) = \pi_m(a_m) = \varepsilon_m(x)$$

Hence $p^n b = x$. Thus $x \in p^n\mathbb{Z}_p$. ☐

Proposition – $\mathbb{Z}_p$ is a local ring, decomposition of non-zero elements
If $x \in \mathbb{Z}_p$ then

1. $x_n \in A_n$ is a unit if and only if $x_n \notin pA_n$.
2. $x \in \mathbb{Z}_p$ is a unit if and only if $x \notin p\mathbb{Z}_n$.
3. For any $x \in \mathbb{Z}_p \setminus \{0\}$ there exist unique $n \in \mathbb{N}$ and $u \in \mathbb{Z}_p$ such that u is a unit and $p^n u = x$.

Proof.

1. If x_n is a unit and $x_n \in pA_n$ then write $x_n = py_n$ for $y_n \in A_n$. We see that p is a unit since $x_n^{-1} py_n = 1$. However p is nilpotent since $p^n = 0$ a contradiction. Hence $x_n \notin pA_n$. Conversely if $x_n \notin pA_n$ then supposing $x_1 = 0$ deduces $x \in p\mathbb{Z}_p$ by the previous proposition. Hence $x_n \in pA$ a contradiction. Thus $x_1 \neq 0 \in A_1$, a field, so x_1 is a unit in A_1. Hence there exist $x_\mathbb{Z}, y_\mathbb{Z}, z_\mathbb{Z} \in \mathbb{Z}$ such that $\iota(x_\mathbb{Z}) = x$ and

$$\begin{aligned} x_\mathbb{Z} y_\mathbb{Z} + pz_\mathbb{Z} =& 1 \\ \Rightarrow \pi_n(x_\mathbb{Z} y_\mathbb{Z} + pz_\mathbb{Z}) =& 1 \\ \Rightarrow x_n y_n + pz_n =& 1 \\ \Rightarrow x_n y_n (1 + \cdots + (pz_n)^{n-1}) = 1 - (pn)^z = 1 \in A_n & \\ \Rightarrow x_n \text{ is a unit} & \end{aligned}$$

   Hence x_n is a unit if and only if $x_n \notin pA_n$.

2. If x is a unit of $\mathbb{Z}_p$ then in particular x_1 is a unit. Suppose $x \in p\mathbb{Z}_p$ then $x_1 = 0$ by the previous proposition. Hence x_1 is not a unit, a contradiction. Thus $x \notin p\mathbb{Z}_p$.

   For the converse suppose $x \notin p\mathbb{Z}_p$ then by the previous proposition $x_1 \neq 0$. For any $n \in \mathbb{N}$, if $x_n \in A_n$ then $x_1 = \phi_n \circ \cdots \phi_2 x_n = 0$ which is false. Hence for any $n \in \mathbb{N}$, $x_n \notin pA_n$ which by the first part implies there exists a unique $y_n \in A_n$, $x_n y_n = 1$. We show that $y := (y_n)_{n \in \mathbb{N}}$ is the inverse of x in $\mathbb{Z}_p$. To show that $y \in \mathbb{Z}_p$ let $n \in \mathbb{N}$.

$$x_n \phi_{n+1}(y_{n+1}) = \phi_{n+1}(x_{n+1})\phi_{n+1}(y_{n+1})\phi_{n+1}(x_{n+1}y_{n+1}) = \phi(1) = 1$$

   Hence $\phi_{n+1}(y_{n+1}) = y_n$ by uniqueness of inverses in A_n. To show that $xy = 1$ note that for any $n \in \mathbb{N}$, $\varepsilon_n(xy) = x_n x_y = 1$. Hence $xy = 1$.

3. Let $x \in \mathbb{Z}_p$ be non-zero and consider the set

$$\{n \in \mathbb{N} \,|\, \varepsilon_n(x) = 0\}$$

   This is non-empty since $\varepsilon_0(x) = 0$. By induction there exists a maximum of this set, call this n. Since $\varepsilon_n(x) = 0$ by the previous proposition $x = p^n y$ for some $y \in \mathbb{Z}_p$. Suppose $y \in p\mathbb{Z}_p$ then $\varepsilon_{n+1}(x) = 0$ which is a contradiction with maximality. Hence by the previous part of this proposition y is a unit.

   Suppose we have another decomposition $x = p^m z$ with z a unit. Then by maximality of n, $m \leq n$. By the previous proposition we have that multiplication by p^m is injective. Hence $p^n y = p^m z$ implies $p^{n-m} y = z$. Since z is a unit, $n - m = 0$. Hence $n = m$ and $y = p^{n-m} y = z$.

$\square$

Definition – $\mathbb{N}_\infty$
On the set $\mathbb{N}_\infty := \mathbb{N} \cup \{\infty\}$ define commutative addition such that if $n, m \in \mathbb{N}$ then it is the usual addition and for any $x \in \mathbb{N}_\infty$, $x + \infty = \infty$. We order the set using $\leq$, where it is the usual $m \leq n$ for $m, n \in \mathbb{N}$ and for any $x \in \mathbb{N}_\infty$, $x \leq \infty$ and if $\infty \leq x$ then $x = \infty$. This is a total order hence we have a well defined infimum for any non-empty set.

Definition – p-adic valuation
Given p a prime, define $v_p : \mathbb{Z}_p \to \mathbb{N}_\infty$ sending any non-zero x to n, where $n \in \mathbb{N}$ and $u \in \mathbb{Z}_p$ is a unit such that $x = p^n u$. In the other case we define $v_p(0) := \infty$.

Proposition
For any p prime and $x, y \in \mathbb{Z}_p$

$$v_p(xy) = v_p(x) + v_p(y), \quad \inf\{v_p(x), v_p(y)\} \leq v_p(x+y)$$

Proof. Case on what x, y are. □

Corollary
$\mathbb{Z}_p$ is an integral domain.

Proof. Let $x, y \in \mathbb{Z}_p$ be such that $xy = 0$. Suppose for a contradiction both x, y are non-zero. Then $v_p(x), v_p(y) \in \mathbb{N}$ hence $\infty = v_p(xy) = v_p(x) + v_p(y) \in \mathbb{N}$, a contradiction. □

Definition – Metric on $\mathbb{Z}_p$
Define a norm on $\mathbb{Z}_p$ by

$$|\star| : \mathbb{Z}_p \to \mathbb{R}_{\geq 0} := x \mapsto \begin{cases} 0 & , x = 0 \\ p^{-v_p(x)} & , x \neq 0 \end{cases}$$

This satisfies

1. $|x| = 0 \Leftrightarrow x = 0$
2. $|x+y| \leq \max(|x|, |y|) \leq |x| + |y|$
3. $|xy| \leq |x| |y|$
4. $|1| = 1$

This induces a metric on $\mathbb{Z}_p$.

Proof. Straight forward. □

Proposition – Cosets are clopen balls
For any n and $a \in \mathbb{Z}$ the coset $a + p^n\mathbb{Z}_p$ is a clopen ball $B_\delta(a)$ for some $\delta \in \mathbb{R} -> 0$.

Proof. $b \in a+p^n\mathbb{Z}_p$ if and only if $n \leq v_p(b-a)$ if and only if $|b-a| \leq p^{-n}$ if and only if $|b-a| < \frac{p^{-n}+p^{1-n}}{2} =: \delta$, as the image of the norm is discrete. Hence $a + p^n\mathbb{Z}_p = \overline{B_{p^{-n}(a)}} = B_\delta(a)$ and is clopen. □

Proposition – Induced topologies are equivalent
The metric topology $\mathcal{T}_0$ is the same as the subspace topology $\mathcal{T}_1$ from $\prod_{n\in\mathbb{N}} A_n$.

Proof. We first show that the neighbourhoods of points are the same. Call the neighbourhood filter for a point a in the metric tolopogy $N_0(a)$ and the other $N_1(a)$. We use $\langle \star \mid \ldots \rangle$ to mean the neighbourhood filter generated by $\{\star \mid \ldots\}$.

$$\begin{aligned}
N_1(a) &= \langle U \cap \mathbb{Z}_p \mid a \in U \in \text{ product topology on } \prod A_n \rangle \\
&= \langle \varepsilon_n^{-1}(U) \cap \mathbb{Z}_p \mid \exists n \in \mathbb{N}, a_n \in U \subseteq A_n \rangle \\
&= \langle U \subseteq \mathbb{Z}_p \mid \exists n \in \mathbb{N}, a + \ker(\varepsilon_n) \subseteq U \rangle \\
&= \langle U \subseteq \mathbb{Z}_p \mid \exists n \in \mathbb{N}, a + p^n\mathbb{Z}_p \subseteq U \rangle \\
&= \langle U \subseteq \mathbb{Z}_p \mid \exists \delta > 0, B_\delta(a) \subseteq U \rangle \\
&= N_0(a)
\end{aligned}$$

The penultimate equality is due to cosets being clopen balls for one inclusion and the other inclusion follows from finding $n \in \mathbb{N}$ such that $p^{-(n+1)} < \delta < p^{-n}$.

Since a subset U is open in a topology if and only if for all points $a \in U, U \in N(p)$ we see that $U \in \mathcal{T}_0$ if and only if $\forall p \in U, U \in N_0(p)$ if and only if $\forall p \in U, U \in N_1(p)$ if and only if $U \in \mathcal{T}_1$. □

Proposition – Topological properties of $\mathbb{Z}_p$
$\mathbb{Z}_p$ is complete in the topological sense and the image of $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Proof. Any Cauchy sequence in $\mathbb{Z}_p$ has a subsequence converging to $x \in \mathbb{Z}_p$ as $\mathbb{Z}_p$ is a compact metric space. This is also the unique limit of the original sequence as it is Cauchy. Hence $\mathbb{Z}_p$ is complete.

Clearly $\overline{\iota(\mathbb{Z})} \subseteq \mathbb{Z}_p$. Let $x \in \mathbb{Z}_p$. We want to show that there exists a sequence in $\iota(\mathbb{Z})$ converging to x, hence showing that $x \in \overline{\iota(\mathbb{Z})}$. For any $n \in \mathbb{N}$ there exists an element $b \in \mathbb{Z}$ such that $\pi_n(b) = \varepsilon_n(x)$. Define the sequence $y : \mathbb{N} \to \mathbb{Z}_p := n \to \iota(b)$. Then we claim that $\lim_{n\in\mathbb{N}} y(n) = x$ Let $\delta \in \mathbb{R}_{>0}$. There exists $N \in \mathbb{N}$ such that $p^{-N} < \delta$. Let $n \in \mathbb{N}$ be such that $N \leq n$. Then $\varepsilon_n(x - y(n)) = 0$ implies $x - y(n) \in p^n A_n$ and so

$$|x - y(n)| = p^{-v_p(x-y(n))} \leq p^{-n} \leq p^{-N} < \delta$$

Thus the limit exists and is x. Hence $\overline{\iota(\mathbb{Z})} = \mathbb{Z}_p$. □

Definition – $\mathbb{Q}_p$
Since $\mathbb{Z}_p$ is an integral domain, we can construct its field of fractions. We call this $\mathbb{Q}_p$.

Proposition – Inclusions into $\mathbb{Q}_p$
There is a unique injective ring morphism $\mathbb{Z}_p \to \mathbb{Q}_p$ which (without confusion) we treat as $\subseteq$ and there is a unique injective extension of the ring morphism $\iota : \mathbb{Z} \to \mathbb{Z}_p$ to $\mathbb{Q} \to \mathbb{Q}_p$.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\subseteq"] \arrow[d, "\iota"'] & \mathbb{Q} \arrow[d, dashed] \\
\mathbb{Z}_p \arrow[r, "\subseteq"'] & \mathbb{Q}_p
\end{tikzcd}$$

Proof. The inclusion $\mathbb{Z}_p \to \mathbb{Q}_p$ is a result of the construction of the field of fractions. We extend ι by mapping $\frac{a}{b} \in \mathbb{Q}$ to $\frac{\iota(a)}{\iota(b)} \in \mathbb{Q}_p$. Check that it is well-defined and injective, a ring morphism and that the diagram above commutes. $\square$

Proposition
$\mathbb{Q}_p \cong \mathbb{Z}_p[\frac{1}{p}]$ canonically and any unit of $\mathbb{Q}_p$ can be uniquely written in the form $p^n u$ for $n \in \mathbb{Z}$ and u a unit in the image of $\mathbb{Z}_p$ under the isomorphism.

Proof. Let $f : \mathbb{Z}_p[\frac{1}{p}] \to \mathbb{Q}_p$ such that $\sum_{i=0}^n x_i(\frac{1}{p})^i \mapsto \sum_{i=0}^n \frac{x_i}{p^i}$. Clearly f is well defined and injective. To show that it is surjective note that for any element $\frac{a}{b} \in \mathbb{Q}_p$ with $a, b \in \mathbb{Z}_p, b \neq 0$ we can write $b = p^n u$ for unique $n \in \mathbb{N}$ and u a unit. Hence $\frac{a}{b} = \frac{a}{p^n u} = \frac{au^{-1}}{p^n}$ which is due to an element of $\mathbb{Z}_p[\frac{1}{p}]$ via f.

The same trick gives us the decomposition of units in $\mathbb{Q}_p$. $\square$

Definition – p-adic valuation for $\mathbb{Q}_p$
Extend the definition of v_p to $\mathbb{Q}_p$ by taking $x \neq 0$ to n such that $p^n u = x$.

Note that $0 \leq v_p(x)$ if an only if x is a p-adic integer.

Definition – Addition is a homeomorphism on $\mathbb{Q}_p$
Let $a \in \mathbb{Q}_p$. Then the map $\mathbb{Q}_p \to \mathbb{Q}_p$ sending $b \mapsto a + b$ is a homeomorphism.

Proof. Let $b \in \mathbb{Q}_b$ and let $\delta \in \mathbb{R}_{>0}$. It suffices that $a + B_\delta(b) \subseteq B_\delta(a + b)$. Indeed if $c \in B_\delta(b)$ then $|a + c - (a + b)| = |c - b| < \delta$.

This map has inverse $-a$ which is continuous for the same reasons. Hence $a + \star$ is a homeomorphism. $\square$

Proposition – Topological properties of $\mathbb{Q}_p$
Useful properties:

1. For any $n \in \mathbb{N}$, $p^n\mathbb{Z}_p$ is clopen in $\mathbb{Q}_p$, in particular $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$.
2. $\mathbb{Q}_p$ is locally compact and $\iota(\mathbb{Q})$ is dense in $\mathbb{Q}_p$.
3. $\mathbb{Q}_p$ is complete.

Proof. Since $\mathbb{Z}_p$ and $\mathbb{Q}_p$ share the same metric Each $p^n\mathbb{Z}_p$ is clopen in $\mathbb{Q}_p$. We first note that $\mathbb{Q}_p$ is locally compact at 0 since $\mathbb{Z}_p$ is an open compact neighbourhood of 0. Furthermore, for any $a \in \mathbb{Q}_p$, $a + \star$ is a homeomorphism so the coset $a + \mathbb{Z}_p$ is the image of an open compact set which is open and compact. Clearly $a \in a + \mathbb{Z}_p$. Hence $\mathbb{Q}_p$ is locally compact.

Clearly $\overline{\iota(\mathbb{Q})} \subseteq \mathbb{Q}_p$ Let $x \in \mathbb{Q}_p$, then $x = p^n u$ for $n \in \mathbb{N}$ and $u \in \mathbb{Z}_p$ a unit. Then $u \in \overline{\iota(\mathbb{Z})} \subseteq \overline{\iota(\mathbb{Q})}$ and so $x \in p^n\overline{\iota(\mathbb{Q})} \subseteq \overline{\iota(\mathbb{Q})}$. Thus $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

$\mathbb{Q}_p$ is complete: take a Cauchy sequence in $\mathbb{Q}_p$. Let $\delta = 1$, then there exists $N \in \mathbb{N}$ such that for any $n, m \in \mathbb{N}$, if $N \leq n \leq m$ then $|x_m - x_n| \leq 1$. Hence the sequence $(x_m)_{N \leq m} \subseteq x_N + \mathbb{Z}_p$ which is compact as it is an image of the homeomorphism $x_m + \star$. Hence there is a subsequence converging to a limit in $x_m + \mathbb{Z}_p$, and applying Cauchy we conclude this is the limit of the original sequence. ☐

Proposition – Series converge iff terms converge
Let $x : \mathbb{N} \to \mathbb{Q}_p$ be a sequence. Then x converges if and only if $\lim_{n\in\mathbb{N}}(x(n+1) - x(n)) = 0$.

Proof. Since $\mathbb{Q}_p$ is complete it suffices to show that x is Cauchy if and only if $\lim_{n\in\mathbb{N}}(x(n+1) - x(n)) = 0$. The forward implication is straightforward. For the other direction take $\delta \in \mathbb{R}_{>0}$. By assumption

$$\exists N \in \mathbb{N}, \forall n \in \mathbb{N}_{>N}, |x(n+1) - x(n)| < \frac{\delta}{2}$$

Let $n, m \in \mathbb{N}$ be such that $N \leq n \leq m$. By induction we can show that $|x(m) - x(n)| \leq \frac{\delta}{2} < \delta$, using $|x + y| \leq \max(|x|, |y|)$ for the induction. ☐

2.2 p-adic Equations

Proposition – Non-empty projective limits
Suppose $F : (\mathbb{N}, \leq) \to \mathcal{C}$ is a projective system. Denote $\downarrow^n_m$ as the image map in $\mathcal{C}$ from $F(n) \to F(m)$. Suppose that for every $n \in \mathbb{N}$ the object $F(n)$ in $\mathcal{C}$ is finite and non-empty. Then the projective limit

$$\varprojlim F := \left\{ x \in \prod_{n\in\mathbb{N}} F(n) \,|\, \forall n \in \mathbb{N}, \downarrow^n_{n+1} x_{n+1} = x_n \right\}$$

is non-empty. Conversely if the projective limit is non-empty then each $F(n)$ is non-empty.

Proof. The trick is to construct a surjective projective system where the image objects are subsets of each $F(n)$. Let $n \in \mathbb{N}$. Suppose for a contradiction that

$$\forall k \in \mathbb{N}, \exists l \in \mathbb{N}_{\geq k}, \downarrow_n^{n+l} D_{n+l} \neq \downarrow_n^{n+k} D_{n+k}$$

Then by induction we can show that

$$\forall k \in \mathbb{N}, \exists l \in \mathbb{N}_{\geq k}, \downarrow_n^{n+l} D_{n+l} \subset \downarrow_n^{n+k} D_{n+k}$$

Since D_n is finite and each $\downarrow_n^{n+k} D_{n+k} \subseteq D_n$, we can conclude by induction that there exists $k \in \mathbb{N}$ such that $\downarrow_n^{n+k} D_{n+k} = \varnothing$, which implies that D_{n+k} is empty, a contradiction. Hence

$$\exists k \in \mathbb{N}, \forall l \in \mathbb{N}_{\geq k}, \downarrow_n^{n+l} D_{n+l} = \downarrow_n^{n+k} D_{n+k}$$

The sets 'become constant'. We define a functor $G : (\mathbb{N}, \leq) \to \mathcal{C}$ sending $n \mapsto \downarrow_n^{n+k} D_{n+k}$ and with the same image maps as F. This functor is well-defined and surjective because for any $n \in \mathbb{N}$, using the 'becomes constant' property of $G(n+1)$ we can show that $\downarrow_n^{n+1} G(n+1) = G(n)$.

Let $x_0 \in G(0)$, which is non-empty as it is the image of a non-empty set $g(k)$ for some $k \in \mathbb{N}$. By induction we can find $x_n \in G(n)$ for each $n \in \mathbb{N}$ such that $\downarrow_n^{n+1} x_{n+1} = x_n$. Hence $(x_n)_{n\in\mathbb{N}} \in \varprojlim G$. Since each $x_n \in F(n)$, $(x_n)_{n\in\mathbb{N}} \in \varprojlim F$.

The converse is immediate from the previous proposition. □

Notation. *For $\phi : A \to B$ a ring morphism, S a finite subset of $A[x_1, \ldots, x_m]$, and*

$$f = \sum_{\lambda \in S} \lambda \prod_{i=1}^{m} (x_i)^{r_{i,\lambda}} \quad \in A[x_1, \ldots, x_m]$$

we write $\phi(f)$ to mean

$$\sum_{\lambda \in S} \phi(\lambda) \prod_{i=1}^{m} (x_i)^{r_{i,\lambda}} \quad \in B[x_1, \ldots, x_m]$$

Proposition – Vanishing commutes with limit
Let $I \subseteq \mathbb{Z}_p[x_1, \ldots, x_m]$. Then

$$\mathbb{V}(I, \mathbb{Z}_p) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{V}(\varepsilon_n(I), A_n)$$

via $(a_1, \ldots, a_m) \in \mathbb{V}(I)$ being sent to $(\varepsilon_n(a_1), \ldots, \varepsilon_n(a_m))_{n\in\mathbb{N}} \in \varprojlim \mathbb{V}(\varepsilon_n(I), A_n)$.

In particular $\mathbb{V}(I)$ is non-empty if and only if for all $n \in \mathbb{N}$, $V_n := \mathbb{V}(\varepsilon_n(I))$ is non-empty, where $\varepsilon_n(I)$ denotes $\{\varepsilon_n(f) \mid f \in I\}$.

Proof. Note that $(a_1, \ldots, a_m) \in (\mathbb{Z}_p)^m$, if and only if for all $i \in \{1, \ldots, m\}$, $a_i \in \varprojlim A_n$ if and only if for all $i \in \{1, \ldots, m\}$, $n \in \mathbb{N}$, $\varepsilon_n(a_i) \in A_n$ and $\downarrow_n^{n+1} \varepsilon_{n+1}(a_i) = \varepsilon_n(a_i)$. This is if and only if for all $n \in \mathbb{N}$,

$$(\varepsilon_n(a_1), \ldots, \varepsilon_n(a_m)) \in A_n^m \text{and} \downarrow_n^{n+1} (\varepsilon_{n+1}(a_1), \ldots, \varepsilon_{n+1}(a_m)) = \varepsilon_n(a_i)$$

which is if and only if $(\varepsilon_n(a_1), \ldots, \varepsilon_n(a_m))_{n\in\mathbb{N}} \in \varprojlim(A_n^m)$. Hence we have an isomorphism of rings

$$(\mathbb{Z}_p)^m = (\varprojlim A_n)^m \cong \varprojlim(A_n^m)$$

We first show that the functor V mapping $n \mapsto V_n$ and $n \leq m$ to $\downarrow_n^m\colon V_m \to V_n$ is a projective system. We just need to show that

$$\forall n \in \mathbb{N}, \forall a \in V_{n+1}, \downarrow_n^{n+1} a \in V_n$$

Indeed if $a \in V_{n+1}$ then [1]

$$\begin{aligned}
\varepsilon_n(f)\circ \downarrow_n^{n+1} (a) &= \downarrow_n^{n+1} \circ \varepsilon_{n+1}(f)(\downarrow_n^{n+1} (a)) & \\
&= \downarrow_n^{n+1} (\varepsilon_{n+1}(f)(a)) & \text{verify this} \\
&= \downarrow_n^{n+1} (0) = 0 & \text{since } a \in V_{n+1}
\end{aligned}$$

Hence this forms a projective system with each V_n finite (since they are respectively subsets of A_n).

Claim: $\varprojlim V$ is isomorphic to $\mathbb{V}(I)$ via the isomorphism

$$(\mathbb{Z}_p)^m \cong \varprojlim(A_n^m)$$

$$\begin{aligned}
(a_1, \ldots, a_m) \in \mathbb{V}(I) \subseteq (\mathbb{Z}_p)^m &\Leftrightarrow \forall f \in I, f(a_1, \ldots, a_m) = 0 \in \mathbb{Z}_p \\
&\Leftrightarrow \forall n \in \mathbb{N}, \forall f \in I, \varepsilon_n(f(a_1, \ldots, a_m)) = 0 \in A_n \\
&\Leftrightarrow \forall n \in \mathbb{N}, \forall f \in I, \varepsilon_n(f)(\varepsilon_n(a_1), \ldots, \varepsilon_n(a_m)) = 0 \in A_n \\
&\Leftrightarrow (\varepsilon_n(a_1), \ldots, \varepsilon_n(a_m))_{n\in\mathbb{N}} \in \varprojlim V
\end{aligned}$$

□

Definition

For R a ring $(a_1, \ldots, a_m) \in R^m$ is primitive if there exists $i \in \{1, \ldots, m\}$ such that a_i is a unit. For the cases $R = A_n$ or $R = \mathbb{Z}_p$, elements are non-primative if and only if for all $i \in \{1, \ldots, m\}$, $a_i \in pR^m$.

Proposition

Let $I \subseteq \mathbb{Z}_p[x_1, \ldots, x_m]$ be such that $\forall f \in I, f$ is homogeneous. Then the following are equivalent:

1. There exists a non-zero $a \in \mathbb{V}(I, \mathbb{Q}_p)$.
2. There exists a primitive $a \in \mathbb{V}(I, \mathbb{Z}_p)$.
3. For each $n \in \mathbb{N}$, there exists a primitive $a \in \mathbb{V}(\varepsilon_n(I), A_n)$.

[1] For $\phi : A \to Bwe$ and $a \in A^m$ we write $\phi(a) = \phi(a_1, \ldots, a_m) = (\phi(a_1), \ldots, \phi(a_m))$. In our projective system we use this notation for $\downarrow_n^{n+1}$.

Proof. 2. implies 1. is straightforward. If 1. is true then there exists a non-zero $a = (a_1, \dots, a_m) \in (\mathbb{Q}_p)^m$ such that for any $f \in I$, $f(a) = 0$. Define $b = p^{-h}a$ where $h = \min_{1 \le i \le m}(v_p(a_i))$. This is well-defined as all a_i are non-zero. b is in $(\mathbb{Z}_p)^m$: for any $i \in \{1, \dots, m\}$, $a_i = p^{v_p(a_i)}u_i$ for a unit $u_i \in \mathbb{Z}_p$ and so $b_i = p^(v_p - h)u_i$ with $0 \le v_p - h = v_p(b_i)$ since h was the minimum. b is primitive: there exists an i that minimises $v_p(a_i)$. Then $b_i = p^{-h}a_i = p^{v_p(a_i)-h}u_i = u_i$ is a unit in $\mathbb{Z}_p$. b is in the vanishing $\mathbb{V}(I, \mathbb{Z}_p)$ because f is homogeneous. (Write out f as a sum and use the fact that the powers add to the degree of f.)

We show 2. if and only if 3. by considering the subsets $P(I, \mathbb{Z}_p)$ and $P(\varepsilon_n(I), A_n)$, the primitive elements of the vanishings. The $P(\varepsilon_n(I), A_n)$ form a projective system with limit $\varprojlim P(\varepsilon_n(I), A_n) \cong P(I, \mathbb{Z}_p)$ via the same isomorphism. Then $P(I, \mathbb{Z}_p)$ is non-empty if and only if for all $n \in \mathbb{N}$, $P(\varepsilon_n(I), A_n)$ is non-empty. □

Proposition – Taylor's theorem
If R be a ring, $f \in R[x]$ and $a \in \mathbb{Z}_p$, there exists a $g \in R[x]$ such that

$$f(x) - f(a) = f'(a)(x - a) + g(x)(x - a)^2$$

Proof. Rephrase the statement as

$$f(x) - f(a) = f'(a)(x - a) \quad \mod (x - a)^2$$

We show that for any n, $f = x^n$ satisfies the above. If $n = 0$ then we can pick $g(x) = 0$ and we are done. For the induction step we assume there exists $g \in R[x]$ such that

$$x^n - a^n = na^{n-1}(x - a) + g(x)(x - a)^2$$

Suffices to show that

$$\frac{x^{n+1} - a^{n+1}}{x - a} = (n+1)a^n \quad \mod (x - a)$$

Then

$$\begin{aligned}\frac{x^{n+1} - a^{n+1}}{x - a} &= x^n + \dots + a^n \\ &= \sum_{k=0}^{n} x^k a^{n-k} \quad \mod (x - a)^2 \\ &= \sum_{k=0}^{n} a^n \quad \mod (x - a)^2 \\ &= (n+1)a^n \quad \mod (x - a)^2\end{aligned}$$

Hence it is true for all monomials. Now let $f = \sum_n \lambda_n x^n$ be any polynomial. Then

$$f(x) - f(a) = \sum_n \lambda_n (x^n - a^n) \quad \mod (x - a)^2$$

$$\begin{aligned}&= \sum_n \lambda_n n a^{n-1}(x - a) \quad \mod (x - a)^2 \\ &= (x - a)\sum_n \lambda_n n a^{n-1} \quad \mod (x - a)^2 \\ &= (x - a)f'(a) \quad \mod (x - a)^2\end{aligned}$$

∎

Proposition – Newton's Method
Let $f \in \mathbb{Z}_p[x]$, $a \in \mathbb{Z}_p$ conceptually: Suppose for $f'(a) \leq 1$. Then there exists $y \in \mathbb{Z}_p$ such that

1. $|f'(a)(y-a)| \leq |f(a)|$
2. $|f(y)| \leq \frac{|f(a)|}{p}$
3. $|f'(y)| = |f'(a)|$

Hence we have y such that it is close to a, $f(y)$ is 'much' closer to 0, and the derivative is the same size.

Elementarily: Suppose $b, c \in \mathbb{Z}_p, n, k \in \mathbb{Z}$. Suppose $0 \leq 2k < n$, $f(a) = p^n b$, $f'(a) = p^k c$ and c is a unit. Then there exists $y \in \mathbb{Z}_p$ such that

$$y - a \in p^{n-k}\mathbb{Z}_p \quad f(y) \in p^{n+1}\mathbb{Z}_p, \quad v_p(f'(y)) = k,$$

Proof. Take $y = a - p^{n-k}c^{-1}b$. Clealy $y - a \in p^{n-k}\mathbb{Z}_p$. By Taylor's formula

$$\begin{aligned} f(y) - f(a) &= -f'(a)p^{n-k}c^{-1}b + g(y)c^{-2}b^2(p^{n-k})^2 \\ \Rightarrow f(y) - p^n b &= -p^k b p^{n-k} z + g(y)c^{-2}b^2 p^{2n-2k} \\ \Rightarrow f(y) &= c^{-2}b^2 g(y)p^{2n-2k} \end{aligned}$$

Hence $f(y) \in p^{2n+1}\mathbb{Z}_p$ if and only if $2n + 1 \leq 2n - 2k$ if and only if $2k + 1 \leq n$, which is true.

To check that $v_p(f'(y)) = k$ we use Taylor's formula again:

$$f'(y) - f'(a) = f''(a)(y-a) + g(y)(y-a)^2$$

Hence

$$\begin{aligned} f'(y) &= f'(a) - f''(a)p^{n-k}c^{-1}b + g(x)p^{2n-2k}c^{-2}b^2 \\ &= p^k c - (f''(a)c^{-1}b + g(x)p^{n-k}c^{-2}b^2)p^{n-k} \\ &= p^k(c - \star p^{n-2k}) \end{aligned}$$

where $\star \in \mathbb{Z}_p$. Hence $c - \star p^{n-2k}$ is a unit since p does not divide it. Thus $v_p(f'(y)) = k$. ∎

Proposition – Polynomials are continuous
The maps $\star + \star : (\mathbb{Q}_p)^2 \to \mathbb{Q}_p$ and $\star \cdot \star : (\mathbb{Q}_p)^2 \to \mathbb{Q}_p$ are continuous. Hence by induction polynomials are continuous maps.

Proof. Standard. For product use the trick

$$ab - cd = a(b-d) + b(a-c) + (a-c)(d-b)$$

∎

Proposition – General Hensel
If $f \in \mathbb{Z}_p[x_1, \dots, x_m]$ and there exist $a \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ such that $0 \leq 2k < n$ and $f(a) \in p^n\mathbb{Z}_p$ and there exists $j \in \{1, \dots, m\}$ such that $v_p(\frac{\partial f}{\partial x_j}(a)) = k$, then there exists $y \in (\mathbb{Z}_p)^m$ such that

$$a - y \in p^{n-k}\mathbb{Z}_p \quad \text{and} \quad f(y) = 0$$

Proof. Case $m = 1$ and let $f \in \mathbb{Z}_p[x_1]$, $a \in \mathbb{Z}_p, n, k \in \mathbb{Z}$ such that $f(a) \in p^n\mathbb{Z}_p$ such that $v_p(\frac{\partial f}{\partial x_1}(a)) = v_p(f'(a)) = k$. Let $y_n = a$. By induction with Newton's Method at each step, we obtain for each $l \in \mathbb{N}_{>n}$ a $y_l \in \mathbb{Z}_p$ such that $f(y_l) \in p^m\mathbb{Z}$, $v_p(f'(y_m)) = k$ and $y_l - y_{l-1} \in p^{l-1-k}\mathbb{Z}_p$. The $(y_m)_{m\in\mathbb{N}}$ is a sequence in $\mathbb{Z}_p$ which is Cauchy since each $y_l - y_{l-1} \in p^{l-1-k}\mathbb{Z}_p$ so $|y_l - y_{l-1}| \leq p^{k+1-l} \to 0$ as $l \to \infty$. Since $\mathbb{Z}_p$ is complete this converges to $y \in \mathbb{Z}_p$. It is clear that $|y - yl| \leq p^{k-l}$ for each l. In particular $|y - a| \leq p^{k-n}$ hence $a - y \in p^{n-k}$. Furthermore since f is continuous and $f(y_n)$ are in shrinking balls around 0,

$$f(y) = f(\lim_{n\to\infty} y_n) = \lim_{n\to\infty} f(y_n) = 0$$

For the case $1 < m$ we reduce it to the same situation as above. Suppose $f \in \mathbb{Z}_p[x_1, \dots, x_m]$, $a \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ such that $f(a) \in p^n\mathbb{Z}_p$ and there exists $j \in \{1, \dots, m\}$ such that $v_p(\frac{\partial f}{\partial x_j}(a)) = k$. Then take $f(a_1, \dots, a_{j-1}, x_j, a_{j+1}, \dots, a_m) \in \mathbb{Z}_p[x_j]$, f with its variables substituted for a_i except for when $i = j$. This satisfies the conditions of the first part so we are done. □

Corollary – Hensel
Let $f \in \mathbb{Z}_p[x_1, \dots, x_m]$, suppose there exists $c \in (p\mathbb{Z}_p)^m$ such that $\varepsilon_1(f(c)) = 0$ and there exists a $j \in \{1, \dots m\}$ such that $\frac{\partial f}{\partial x_j}(c) \neq 0$ then there exists a $c^* \in (\mathbb{Z}_p)^m$ such that $f(c^*) = 0$ and $\varepsilon_1(c^* - c) = 0$.

Proof. Apply general Hensel with $n = 1$ and $k = 0$. □

Corollary – Quadratic forms for $p \neq 2$
Suppose $p \neq 2$, $A \in (p\mathbb{Z}_p)^{n\times n}$ such that for all $i, j \in \{1, \dots, m\}$, $A_{ij} = A_{ji}$ and $\det A$ a unit. Let

$$f = x^T Ax = \sum_{i=1}^{m}\sum_{j=1}^{m} A_{ij}x_ix_j \in \mathbb{Z}_p[x_1, \dots, x_m]$$

If for any $a \in \mathbb{Z}_p$, there exists primitive $c \in (\mathbb{Z}_p)^m$ such that $ep_1(f(c)-a) = 0$ then there exists $c^* \in (\mathbb{Z}_p)^m$ such that $f(c^*) = 0$ and $\varepsilon_1(c^* - c) = 0$.

Proof. By Hensel applied to $g(x) := f(x) - a$ it suffices to show that there exists a $j \in \{1, \dots, m\}$ such that $\frac{\partial f}{\partial x_j}(c) \neq 0$. Suppose not. Then for any $j \in \{1, \dots, m\}$

$$0 = \frac{\partial f}{\partial x_j}(c) = 2\sum_{i\in S} A_i j c_i$$

Since $p \neq 2$ we have that for all j

$$0 = \sum_{i \in S} \varepsilon_1(A_i j)\varepsilon_1(c_i) = \varepsilon_1(A_j)\varepsilon_1(c)$$

Hence

$$0 = \varepsilon_1(A)\varepsilon_1(c)$$

Since the determinant of A is a unit, the determinant of $\varepsilon_1(A)$ is a unit (determinant commutes with ring morphisms). Thus multiplying by the adjugate of $\varepsilon_1(A)$ we obtain $0 = \varepsilon_1(c)$. This is a contradiction as c is primitive. □

Corollary – Quadratic forms for $\mathbb{Z}_2$
Suppose $A \in (2\mathbb{Z}_2)^{n\times n}$ such that for all $i, j \in \{1, \ldots, m\}, A_{ij} = A_{ji}$. Let

$$f = x^T A x = \sum_{i=1}^{m}\sum_{j=1}^{m} A_{ij}x_i x_j \in \mathbb{Z}_2[x_1, \ldots, x_m]$$

If for any $a \in \mathbb{Z}_2$, there exists primitive $c \in (\mathbb{Z}_2)^m$ such that $ep_3(f(c) - a) = 0$ and

$$\det(A) \text{ is a unit of } \mathbb{Z}_2 \quad \vee \quad \exists j \in \{1, \ldots, m\}, \varepsilon_2(\frac{\partial f}{\partial x_j}(c)) \neq 0$$

then there exists $c^* \in (\mathbb{Z}_p)^m$ such that $f(c^*) = 0$ and $\varepsilon_1(c^* - c) = 0$.

Proof. We show that

$$\det A \text{ is a unit of } \mathbb{Z}_2 \quad \Rightarrow \quad \exists j \in \{1, \ldots, m\}, \varepsilon_2(\frac{\partial f}{\partial x_j}(c)) \neq 0$$

Suppose not.

$$\begin{aligned}
&\forall j \in \{1, \ldots, m\}, \varepsilon_2(\frac{\partial f}{\partial x_j}(c)) = 0 \\
&\Rightarrow \forall j, \varepsilon_2(2\sum A_{ij}c_i) = 0 \\
&\Rightarrow \forall j, 2\varepsilon_2(A_j)\varepsilon_2(c) = 0 \\
&\Rightarrow 2\varepsilon_2(A)\varepsilon_2(c) = 0 \\
&\Rightarrow 2\varepsilon_2(c) = 0 \quad \text{since } \det A \text{is a unit} \\
&\Rightarrow \varepsilon_2(c) = 0 \vee \varepsilon_2(c) = 2 \qquad\qquad \Rightarrow \varepsilon_1(c) = 0 \quad \text{a contradiction}
\end{aligned}$$

Hence in either case $\exists j, \varepsilon_2(\frac{\partial f}{\partial x_j}(c)) \neq 0$ We can then apply general Hensel with $n = 3, k < 2, g(x) = f(x) - a$ and obtain c^*. □

2.3 Multiplicative group $\mathbb{Q}_p^*$

Definition – $\mathbb{U}_n$
For each $n \in \mathbb{N}$ the map $\varepsilon_n : \mathbb{Z}_p \to A_n$ is a surjective ring homomorphism, thus makes sense to consider $\varepsilon_n : \mathbb{Z}_p^* \to A_n^*$ the surjective group homomorphism of the unit groups. We define the subgroup $\mathbb{U}_n := \ker \varepsilon_n$. We can characterise $\mathbb{U}_n = 1 + p^n\mathbb{Z}_p$ because

$$x \in \mathbb{U}_n \Leftrightarrow \varepsilon_n(x-1) = 0 \Leftrightarrow x - 1 \in p^n\mathbb{Z}_p$$

Note that $\mathbb{U} := \mathbb{U}_0 = \mathbb{Z}_p^*$ and $\mathbb{U}_0/\mathbb{U}_1 = \mathbb{Z}_p^*/\ker \varepsilon_1 \cong \mathbb{F}_p^*$ hence $\mathbb{U}_0/\mathbb{U}_1$ is cyclic and of order $p-1$.

Proposition
For any $n \in \mathbb{N}$, there is a unique group homomorphism $\mathbb{U}_{n+1} \to \mathbb{U}_n$ such that

$$\begin{tikzcd}
A_{n+1}^* \arrow[r, "\downarrow_n^{n+1}"] \arrow[d, "\cong"] & A_n^* \arrow[d, "\cong"] \\
\mathbb{U}/\mathbb{U}_{n+1} \arrow[r] & \mathbb{U}/\mathbb{U}_n
\end{tikzcd}$$

commutes, since each A_n^* is isomorphic to $\mathbb{U}/\mathbb{U}_n$. Thus $\mathbb{U}/\mathbb{U}_n$ form a projective system with limit

$$\varprojlim \mathbb{U}/\mathbb{U}_n \cong \varprojlim A_n^* = \mathbb{U}$$

Without confusion, we label the maps $\mathbb{U}/\mathbb{U}_{n+1} \to \mathbb{U}/\mathbb{U}_n$ by $\downarrow_n^{n+1}$ as well.

Proposition
For any $n \in \mathbb{N}$ the map $\mathbb{U}_n/\mathbb{U}_{n+1} \to \mathbb{Z}/p\mathbb{Z}$ sending $\overline{1 + p^n x} \mapsto \varepsilon_1(x)$ is a group isomorphism. Hence if $m \leq n \in \mathbb{N}$ then $|\mathbb{U}_m/\mathbb{U}_n| = p^{n-m}$.

Proof. The map is well defined: suppose $\overline{1 + p^n x} = \overline{1 + p^n y}$ then there exists a $z \in \mathbb{Z}_p$ such that

$$\frac{1 + p^n x}{1 + p^n y} = 1 + p^{n+1}z$$

Hence $p^n(x - y) = p^{n+1}z(p^n y + 1)$ and so $\varepsilon_1(x - y) = 0$. The map is injective since

$$\varepsilon_1(x - y) = 0 \Rightarrow x - y = pz \Rightarrow 1 + p^n x - (1 + p^n y) = p^n z \Rightarrow \overline{1 + p^n x} = \overline{1 + p^n y}$$

The map is a group morphism because

$$\overline{1 + p^n x 1 + p^n x} = \overline{1 + p^n(x + y + p^n xy)} \mapsto \varepsilon_1(x + y) = \varepsilon_1(x) + \varepsilon_1(y)$$

Note that this gives us $|\mathbb{U}_n/\mathbb{U}_{n+1}| = p$.

Fix m and induct on n. Assume $|\mathbb{U}_m/\mathbb{U}_n| == p^{n-m}$. By the third isomorphism:

$$\mathbb{U}_m/\mathbb{U}_n \cong (\mathbb{U}_m/\mathbb{U}_{n+1})/(\mathbb{U}_n/\mathbb{U}_{n+1})$$

Hence

$$|\mathbb{U}_m/\mathbb{U}_{n+1}| = |\mathbb{U}_m/\mathbb{U}_n|\,|\mathbb{U}_n/\mathbb{U}_{n+1}| = p^{n-m}p = p^{n+1-m}$$

□

Proposition
Suppose $0 \to A \to G \to B \to 0$ is an exact sequence of finite abelian groups. $|A|, |B|$ coprime. Then $G \cong A \bigoplus B$ and there is a unique subgroup of G isomorphic to B given by the kernel of $b : G \to G := x \to |B|x$.

Proof. By injectivity of f It suffices to show that $f(A) \bigoplus \ker(b)$ and $\ker(b) \cong B$. Since $|A|, |B|$ coprime there exist $\lambda, \mu \in \mathbb{N}$ such that $\lambda|A| + \mu|B| = 1$.

$$x \in f(A) \cap \ker(b) \Rightarrow |A|x = |B|x = 0 \Rightarrow x = \lambda|A|x + \mu|B|x = 0$$

Thus the intersection is trivial. For all $y \in G$, $|B|y \in \ker(g) = f(A)$ by exactness. Furthermore $|B|y \in f(A)$ so $|A||B|y = 0$, hence $|A|y \in \ker(b)$. Thus

$$x \in G \Rightarrow x = \lambda|A|x + \mu|B|x$$

where $\lambda|A|x \in \ker(b)$ and $\mu|B|x \in f(A)$. Hence $f(A) \bigoplus \ker(b)$.

$[|_g]\ker(b)$ is well-defined. It is surjective since g is surjective and anything that maps to B under g will have order dividing $|B|$. It is injective because

$$x \in \ker(g) \Leftrightarrow x \in f(A)|B|x = 0 \Leftrightarrow x \in f(A) \cap \ker(b) \Leftrightarrow x = 0$$

Thus this is an isomorphism.

If $B' \leq G$ is isomorphic to B then $|B|B' = 0$ and so $B' \subseteq \ker(b)$ hence they are equal because they have the same finite cardinality. Thus the subgroup isomorphic to B. □

Proposition – $\mathbb{U} = \mathbb{V} \bigoplus \mathbb{U}_1$
$\mathbb{U} = \mathbb{V} \bigoplus \mathbb{U}_1$ where $\mathbb{V} = \left\{x \in \mathbb{U} \,|\, x^{p-1} = 1\right\}$ is the unique subgroup of $\mathbb{U}$ isomorphic to $\mathbb{F}_p^*$.

Proposition
For each $n \in \mathbb{N}$ consider

$$1 \to \mathbb{U}_1/\mathbb{U}_n \to \mathbb{U}/\mathbb{U}_n \to \mathbb{F}_p^* \to 1$$

where the second map an injection is induced by $\mathbb{U}_1 \subseteq \mathbb{U}_n$, and the third a surjection by $\mathbb{U}/\mathbb{U}_n \cong A_n^* \to A_1^* = \mathbb{F}_p^*$.

Calling the second map f and the third map g, let $y = \overline{1+x} \in \mathbb{U}/\mathbb{U}_n$ for $x \in \mathbb{Z}_p$

$$y \in f(\mathbb{U}_1/\mathbb{U}_n) \Leftrightarrow 1 + x \in \mathbb{U}_1 \Leftrightarrow \overline{x} \in p\mathbb{Z}_p \Leftrightarrow y - 1 \in p\mathbb{Z}_p \Leftrightarrow g(y) = 1$$

Hence the above is an exact sequence with $\mathbb{U}_1/\mathbb{U}_n$ and $\mathbb{F}_p^*$ both finite due to our previous computation.

By the previous proposition there exists $\mathbb{V}_n$ a unique subgroup of $\mathbb{U}/\mathbb{U}_n$ isomorphic to $\mathbb{F}_p^*$ and $\mathbb{U}/\mathbb{U}_n \cong \mathbb{U}_1/\mathbb{U}_n \bigoplus \mathbb{F}_p^*$.

Then the $\mathbb{V}_n$ form a projective system with maps $\mathbb{V}_{n+1} \to \mathbb{V}_n$ induced by the maps $\mathbb{U}/\mathbb{U}_{n+1} \to \mathbb{U}/\mathbb{U}_n$:

$$\begin{tikzcd}
A_{n+1} \arrow[r] \arrow[d] \arrow[rr, bend left, "\downarrow_1^{n+1}"] & \mathbb{U}/\mathbb{U}_n \arrow[d] \arrow[dr] & & \mathbb{V}_{n+1} \arrow[dl, "\cong"'] \arrow[dd, dashed] \\
 & & \mathbb{F}_p^* & \\
A_n \arrow[r] \arrow[rr, bend right, "\downarrow_1^{n}"'] & \mathbb{U}/\mathbb{U}_n \arrow[ur] & & \mathbb{V}_n \arrow[ul, "\cong"]
\end{tikzcd}$$

Since the whole diagram commutes (the right triangle commutes because it uses same maps as the middle triangle) the map from $\mathbb{V}_{n+1} \to \mathbb{V}_n$ is well defined and an isomorphism.

Taking the limit of the projective system $\mathbb{V}_n$, we obtain

$$\mathbb{F}_p^* \cong \varprojlim \mathbb{V}_n \leq \varprojlim \mathbb{U}/\mathbb{U}_n \cong \mathbb{U}$$

Furthermore

$$\mathbb{U} \cong \varprojlim \mathbb{U}/\mathbb{U}_n \cong \varprojlim(\mathbb{U}_1/\mathbb{U}_n \bigoplus \mathbb{F}_p^*)$$

Since projective limits commute with direct sums we have that

$$\mathbb{U} \cong \varprojlim(\mathbb{U}_1/\mathbb{U}_n) \bigoplus \varprojlim \mathbb{F}_p^* \cong \mathbb{U}_1 \bigoplus \mathbb{F}_p^*$$

There are at most $x \in \mathbb{Z}_p$ that satisfy $x^{p-1} = 1$ (by sending the polynomial to $\mathbb{Q}_p$ and using factor theorem). There at at least $p-1$ solutions due to the existence of a subgroup isomorphic to $\mathbb{F}_p^*$ and using Lagrange. Hence $\mathbb{V}$ is the unique subgroup isomorphic to $\mathbb{F}_p^*$.