MULTIPLICATIVE GROUPS OF P-ADIC FIELDS

JAMES FAVILLE

1. Introduction

In this section we examine the properties of a map $M_p : \mathbb{Z} \mapsto \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ with the aim of motivating the construction of the p-adic integers $\mathbb{Z}_p$. The particular example of M_p is original to this work; the maps $m_{p,n}$ and the relation on the sequences of im M_p which they describe are taken from Serre [3]. In this section and others, proofs not given citations are original to this paper, though may appear elsewhere in texts not known to the author.

Recall that with respect to a modulus $n \in \mathbb{N}$, every integer $a \in \mathbb{Z}$ is associated with a residue class $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ denoted by $a \pmod n$. We use the notation $a \bmod n$ to denote the least nonnegative residue of $a \pmod n$, which is the unique $b \in \bar{a}$ such that $0 \leq b < n$. More generally, we write $[\bar{a}]$ to denote the least nonnegative element of an equivalency class $\bar{a}$ of integers.

Suppose we are interested in knowing all residues of a particular $a \in \mathbb{Z}$ in moduli $n \in \mathbb{N}$. By the Chinese Remainder Theorem, it suffices to know the residues of a in each prime power p^α. We can represent this information by forming infinite sequences of the residues of a in the powers of each prime p, which we denote by $M_p(a) = (a \pmod p, a \pmod{p^2}, a \pmod{p^3}, \dots)$. A family of maps which are useful in characterizing im M_p is defined below.

Definition 1.1. Define the modular surjection with respect to a prime p as the map $m_{p,n} : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ given by $m_{p,n}(a \pmod p^{n+1}) = a \pmod p^n$. Each $m_{p,n}$ is a homomorphism on the additive and multiplicative groups of $\mathbb{Z}/p^{n+1}\mathbb{Z}$ since for any elements $\bar{a}, \bar{b}$ in the domain with coset representatives a and $b \in \mathbb{Z}$, $m_{p,n}(\bar{a} + \bar{b}) = m_{p,n}(a + b \pmod{n+1}) = a + b \pmod n = a \pmod n + b \pmod n = m_{p,n}(\bar{a}) + m_{p,n}(\bar{b})$. Likewise, $m_{p,n}(\bar{a}\bar{b}) = m_{p,n}(ab \pmod{n+1}) = ab \pmod n = (a \pmod n)(b \pmod n) = m_{p,n}(\bar{a})m_{p,n}(\bar{b})$. Therefore, each $m_{p,n}$ is a ring homomorphism. For any element $\bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$, $\bar{a} = m_{p,n}([\bar{a}] \pmod{p^{n+1}})$, so $m_{p,n}$ is surjective.

Proposition 1.2. *The image of $M_p : \mathbb{Z} \to \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ is exactly the set of sequences x which satisfy these properties.*

Date: Spring 2017, and, in revised form, Fall 2017.

(i) All adjacent terms x_n and x_{n+1} satisfy $m_{p,n}(x_{n+1}) = x_n$.
(ii) There is some $k \in \mathbb{N}$ such that for all integers $n \geq k$, $[x_n] = [x_k]$.

Proof. Let $x = M_p(a)$ denote an arbitrary element of the image of M_p, where $a \in \mathbb{Z}$ is an element of the preimage of x. For every power p^n of p which is greater than a, $a \bmod p^n = a$, so x satisfies (ii). Since every component $a \pmod{p^{n+1}}$ of x is immediately preceded by the component $a \pmod{p^n}$ and $m_{p,n}(a \pmod{p^{n+1}}) = a \pmod{p^n}$, x satisfies (i).

Now let $x = \left(x_n\right)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ denote a sequence for which (i) and (ii) both hold. By (ii), there is some $k \in \mathbb{N}$ such that for all $n \geq k$, $[m_n] = [m_k]$; let us denote by k the *least* index for which this property holds. We claim that x is the image in M_p of $[m_k]$, which we write as $y = M_p([m_k]) = \left(y_n\right)_{n\in\mathbb{N}}$. We immediately know that $x_n = y_n = [m_k] \pmod{p^k}$ for all $n \geq k$ by our choice of k. Now note that since adjacent terms are related by the ring homomorphism $m_{p,n}$, each term of a sequence satisfying (i) completely determines all terms which precede it. Since $x_k = y_k$, $x_n = y_n$ for all $n < k$ as well. Therefore, because we have shown that $x_n = y_n$ for all indices $n \geq k$ and all indices $n < k$, we have shown that $x = y = M_p([m_k])$. □

While property (i) describes an important structural feature of these infinite modular sequences, property (ii) is an artifact of our ability to always find a prime power of p which is greater than the unique integer in the preimage of the sequence. The rest of this paper examines the nature of the mathematical objects which satisfy (i) but not necessarily (ii).

The set of such sequences actually form the integral domain $\mathbb{Z}_p$ of p-adic integers, whose field of fractions is denoted by $\mathbb{Q}_p$. In §2 we construct $\mathbb{Z}_p$ as a inverse limit, and show that its field of fractions $\mathbb{Q}_p$ is well defined. In §3 we further investigate the multiplicative group $\mathbb{Q}_p^\times$, and discuss its isomorphism to more familiar groups.

2. Construction of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

We define an *inverse system* of a ring and an *inverse limit* below, and prove that the inverse limit construction defines a ring. We then proceed to define the p-adic integers $\mathbb{Z}_p$ as the inverse limit of the family $\left(\mathbb{Z}/p^k\mathbb{Z}\right)_{k\in\mathbb{N}}$ of rings whose orders are prime powers of p. This construction of the p-adics is heavily modeled on that of Serre [3, p. 11], which likewise constructs the p-adic integers as an inverse limit by a similar formalism and then defines the field $\mathbb{Q}_p$ as a field of fractions over $\mathbb{Z}_p$. All concepts and proofs from this section are from Serre [3], though often elaborated or simplified for expository purposes, unless indicated otherwise. The proof that $\mathbb{Z}_p$ is an integral domain, however, bears little resemblance to Serre's [3, p. 12] proof,

which sacrifices some directness in order to introduce notation and ideas which are important to his later discussion.

Definition 2.1. A **inverse system** consists of an infinite sequence $\left(A_n\right)_{n\in\mathbb{N}}$ of rings with unity and of a family $\left(\varphi_n : A_{n+1} \to A_n\right)_{n\in\mathbb{N}}$ of onto ring homomorphisms.

Definition 2.2. Given a inverse system $\left(\left(A_n\right)_{n\in\mathbb{N}}, \left(\varphi_n : A_{n+1} \to A_n\right)_{n\in\mathbb{N}}\right)$, the **inverse limit** $\varprojlim_n \left(A_n, \varphi_n\right)$ is the set of all $(a_1, a_2, \dots, a_k, \dots) \in \prod_{n\in\mathbb{N}} A_n$ in the infinite direct product of the rings of the system whose adjacent items a_j and a_{j+1} are related by the associated homomorphism φ_j of the system. Formally, $\varprojlim_n \left(A_n, \varphi_n\right) := \left\{(a_j)_{j\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} A_n : a_j = \varphi_j(a_{j+1}) \text{ for all } j \in \mathbb{N}\right\}$.

We now prove that the inverse limit defines a ring (omitted from Serre [3]).

Theorem 2.3. *Any inverse limit* $\varprojlim_n \left(A_n, \varphi_n\right)$ *is a subring with unity of* $\prod_{n\in\mathbb{N}} A_n$.

Proof. Since $\prod_{n\in\mathbb{N}} A_n$ is a ring and $\varprojlim_n \left(A_n, \varphi_n\right) \subseteq \prod_{n\in\mathbb{N}} A_n$ is a subset of this ring, it remains to be shown that $\varprojlim_n \left(A_n, \varphi_n\right)$ is closed under multiplication and subtraction. Consider first the difference $x - y = \left(x_n - y_n\right)_{n\in\mathbb{N}}$ of two elements $x = (x_n)_{n\in\mathbb{N}}$ and $y = (y_n)_{n\in\mathbb{N}}$ in $\varprojlim_n \left(A_n, \varphi_n\right)$. For any $j \in \mathbb{N}$, $\varphi_j(x_{j+1} - y_{j+1}) = \varphi_j(x_{j+1}) - \varphi_j(y_{j+1}) = x_j - y_j$, so $x - y \in \varprojlim_n \left(A_n, \varphi_n\right)$ and $\varprojlim_n \left(A_n, \varphi_n\right)$ is closed under subtraction. Now consider the product $xy = (x_n y_n)_{n\in\mathbb{N}}$. For any $j \in \mathbb{N}$, $\varphi_j(x_{j+1}y_{j+1}) = \varphi_j(x_{j+1})\varphi_j(y_{j+1}) = x_j y_j$, so $xy \in \varprojlim_n \left(A_n, \varphi_n\right)$, and $\varprojlim_n \left(A_n, \varphi_n\right)$ is closed under multiplication. Let $U \in \prod_{n\in\mathbb{N}} A_n$ denote the multiplicative identity of $\prod_{n\in\mathbb{N}} A_n$, whose nth term is given by the multiplicative identity of A_n. Since each φ_n is a surjective ring homomorphisms, $\varphi_n(1_{n+1}) = 1_n$ for all $n \in \mathbb{N}$, where 1_{n+1} is the unity in A_{n+1} and 1_n is the unity in A_n. Therefore, $U \in \varprojlim_n \left(A_n, \varphi_n\right)$. Because we have shown that $\varprojlim_n \left(A_n, \varphi_n\right)$ is closed under subtraction and multiplication and contains the unity U, we have proven that it is a subring with unity of $\prod_{n\in\mathbb{N}} A_n$. □

We now define the ring of p-adic integers.

Definition 2.4. For a given prime p, the ring $\mathbb{Z}_p$ of **p-adic integers** is the inverse limit of the system defined by the family $\left(\mathbb{Z}/p^n\mathbb{Z}\right)_{n\in\mathbb{N}}$ of rings with power of p orders and by the family $\left(m_{p,n}\right)_{n\in\mathbb{N}}$ of modular surjections.

Remark 2.5. Note that p-adic multiplication is defined componentwise and each component of a p-adic integer is an element of a commutative ring $\mathbb{Z}/p^n\mathbb{Z}$. Consequently, multiplication over $\mathbb{Z}_p$ is commutative. Moreover, $x \in \mathbb{Z}_p$ is the zero element of $\mathbb{Z}_p$ just in case $[x_n] = 0$ for all components x_n of x.

Proposition 2.6. *The image* im M_p *of the mapping discussed in §1 constitutes a subring of* $\mathbb{Z}_p$.

Proof. Since all sequences of im M_p satisfy property (i) of Proposition 1.2, im $M_p \subset \mathbb{Z}_p$, and since $M_p(1)$ is a multiplicative identity in Z_p, im M_p contains the unity of $\mathbb{Z}_p$. Now consider the difference and product of two arbitrary $x = \left(x_n\right)_{n\in\mathbb{N}}$ and nonzero $y = \left(y_n\right)_{n\in\mathbb{N}}$ in the image im M_p. By Proposition 1.2, there is some $k \in \mathbb{N}$ such that $x_j = x_k$ for all $j > k$ and some $l \in \mathbb{N}$ such that $y_j = y_l$ for all $j > l$. Without loss of generality, let us assume that $l < k$. Then for any $j \in \mathbb{N}$ greater than k, the jth component of $x - y$ is given by $x_j - y_j = x_k - y_k$ and the jth component of xy is given by $x_j y_j = x_k y_k$. Therefore, since $x - y$ and xy each define an infinite sequence satisfying properties (i) and (ii) in Proposition 1.1, they are each elements of the image im M_p which is closed under subtraction and multiplication. □

In order to define the field of fractions $\mathbb{Q}_p$, it must first be shown that $\mathbb{Z}_p$ is an integral domain.

Proposition 2.7. *For any* $x = \left(x_n\right)_{n\in\mathbb{N}} \in \mathbb{Z}_p$, *if* $[x_k] = 0$ *for some component* x_k *of* x, *then* $[x_{k-j}] = 0$ *for all previous components* x_{k-j} *with* $j \in \mathbb{N}$ *and* $j < k$.

Proof. Since $x_{k-1} = m_{p,k-1}(x_k) = m_{p,k-1}(0 \pmod{p^k}) = 0 \pmod{p^{k-1}}$, $[x_{k-1}] = 0$. By the principle of mathematical induction, this entails that $[x_{k-j}] = 0$ for all terms x_{k-j} whenever $[x_k] = 0$, as we can induct on $j \in \mathbb{N}$ so long as $k - j > 0$. □

Corollary 2.8. *If an element* $x \in \mathbb{Z}_p$ *is nonzero, then there exists some* $k \in \mathbb{N}$ *such that* $[x_n] \neq 0$ *for all* $n \geq k$.

Proof. Suppose (for contradiction) that $x \in \mathbb{Z}_p$ is nonzero and there existed no such k. Then for an arbitrary component x_n of x, there is some component x_j with $j > n$ such that $[x_j] = 0$. By Prop. 2.7, this entails that $[x_n] = 0$. So we have shown that $x = \left(\bar{0}\right)_{n\in\mathbb{N}}$, which contradicts the hypothesis that x is nonzero. □

Corollary 2.9. $\mathbb{Z}_p$ *is an integral domain.*

Proof. Suppose $xy = 0$ for some $x = \left(x_n\right)_{n\in\mathbb{N}}$ and nonzero $y = \left(y_n\right)_{n\in\mathbb{N}}$. By Cor. 2.8 above, there is some $k \in \mathbb{N}$ such that y_n is nonzero for all indices $n \geq k$. We proceed to prove by contradiction that $[x_n] = 0$ for any arbitrary component x_n of x such that $n > k$.

Suppose $[x_n] \neq 0$. Then since the $(n + k - 1)$th component of xy is 0, p^{n+k-1} must divide $[x_n y_n]$, which means $[x_n] = p^e$ and $[y_n] = p^f$ for nonnegative integer exponents e, f whose sum is divisible by $n + k - 1$. But if $e \geq k$, then since $y_k = [y_n] \pmod{p^k}$, $[y_k] = 0$ which is a contradiction. So $e < k$, which means

$f \geq (n+k-1)-(k-1)$ and $f \geq n$. Therefore, p^n divides $[x_{n+k-1}]$ and $[x_n] = [x_{n+k-1}] \pmod{p^n} = 0$ which is a contradiction.

Since arbitrarily large components of x are zero, by Prop. 2.7 x is zero. Therefore, since $xy = 0$ implies that either x or y is zero for arbitrary $x, y \in \mathbb{Z}_p$, $\mathbb{Z}_p$ is an integral domain. □

Because $\mathbb{Z}_p$ is an integral domain, the field of fractions over $\mathbb{Z}_p$ which is written as $\mathbb{Q}_p$ is well-defined. In §3 below we examine its multiplicative group $\mathbb{Q}_p^\times$.

3. The Multiplicative Group $\mathbb{Q}_p^\times$

Following Serre [3, p. 12], we claim that every nonzero element of $\mathbb{Q}_p$ is of the form $p^e u$ for some $e \in \mathbb{Z}$ and $u \in \mathbb{Z}_p$. We write $p^e q$ for $e \in \mathbb{Z}$ and $q \in \mathbb{Q}_p$ to denote the result of the group action of $\mathbb{Z}$ on $\mathbb{Q}_p$ defined below. Note however that our exposition diverges from that of Serre, who does not discuss group actions.

Proposition 3.1. *The additive group of integers $\mathbb{Z}$ acts on $\mathbb{Q}_p$ by the map $\left(e - f, \frac{x}{y}\right) \mapsto \frac{\left(p^e a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^f b_n \pmod{p^n}\right)_{n\in\mathbb{N}}}$, where each a_n and b_n are coset representatives of the nth coordinates of x and y respectively and $e, f \in \mathbb{N}$.*

Proof. Recall that any integer can be represented as the difference $c - d$ of two nonnegative $c, d \in \mathbb{N}$. To show that the map above is well defined, we prove that $p^{c-d}\frac{x}{y} = p^{e-f}\frac{x}{y}$ for all nonnegative $c, d, e, f \in \mathbb{Z}$ such that $c - d = e - f$ and all $x, y \in \mathbb{Z}_p$ with sequences of coset representatives $\left(a_n\right)_{n\in\mathbb{N}}$ and $\left(b_n\right)_{n\in\mathbb{N}}$ (it is also the case that $p^{e-f}\frac{x'}{y'} = p^{e-f}\frac{x}{y}$ if $\frac{x'}{y'} = \frac{x}{y}$). Note that $p^{c-d}\frac{x}{y} = \frac{\left(p^c a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^d b_n \pmod{p^n}\right)_{n\in\mathbb{N}}}$ and $p^{e-f}\frac{x}{y} = \frac{\left(p^e a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^f b_n \pmod{p^n}\right)_{n\in\mathbb{N}}}$. By definition of a formal fraction, it suffices to show that $\left(p^c a_n \pmod{p^n}\right)_{n\in\mathbb{N}}\left(p^f b_n \pmod{p^n}\right)_{n\in\mathbb{N}} = \left(p^d b_n \pmod{p^n}\right)_{n\in\mathbb{N}}\left(p^e a_n \pmod{p^n}\right)_{n\in\mathbb{N}}$. By componentwise multiplication we calculate $\left(p^{c+f} a_n b_n \pmod{p^n}\right)_{n\in\mathbb{N}}$ on the left side and $\left(p^{d+e} a_n b_n \pmod{p^n}\right)_{n\in\mathbb{N}}$ on the right side. Since $c + f = d + e$, these expressions are equal.

The identity 0 of the additive group $\mathbb{Z}$ is an identity for $\mathbb{Z}$ acting on $\mathbb{Q}_p$ because $p^0\frac{x}{y} = \frac{\left(p^0 a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^0 a_n \pmod{p^n}\right)_{n\in\mathbb{N}}} = \frac{\left(a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(b_n \pmod{p^n}\right)_{n\in\mathbb{N}}} = \frac{x}{y}$ for arbitrary $\frac{x}{y} \in \mathbb{Q}_p$. We now calculate $p^{c-d}(p^{e-f}\frac{x}{y}) = p^{c-d}\frac{\left(p^e a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^f b_n \pmod{p^n}\right)_{n\in\mathbb{N}}} = \frac{\left(p^c p^e a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^d p^f b_n \pmod{p^n}\right)_{n\in\mathbb{N}}} = \frac{\left(p^{c+e} a_n \pmod{p^n}\right)_{n\in\mathbb{N}}}{\left(p^{d+f} a_n \pmod{p^n}\right)_{n\in\mathbb{N}}} = p^{(c+e)-(d+f)}\frac{x}{y} = p^{c-d}p^{e-f}\frac{x}{y}$. Therefore, we have defined an action of $\mathbb{Z}$ on $\mathbb{Q}_p$. □

Lemma. *Any nonzero p-adic integer $x = \left(x_n\right)_{n\in\mathbb{N}}$ can be written as $p^l \chi$ for some $l \in \mathbb{N}$ and any $\chi \in \mathbb{Z}_p^\times$.*

Proof. Recall from the proof of Cor. 2.8 that there must be some greatest power p^k of p which divides a component of x, otherwise arbitrarily large components of x would be zero, which would entail that x itself is 0. Rewrite x as $p^k\chi$ where $[\chi_n]$ is given by $[x_n]/p^e$ and p^e is the largest power of p which divides $[x_n]$. Since all components of χ are divisible by p, their coset representatives are relatively prime to p^n and therefore they are elements of the units $\mathbb{Z}/p^n\mathbb{Z}$. Since all components of χ are therefore invertible, $\chi \in \mathbb{Z}_p^\times$. □

Corollary 3.2. *Any $\frac{x}{y} \in \mathbb{Q}_p$ can be written as $p^e\frac{\chi}{\upsilon}$ for some $e \in \mathbb{Z}$ and p-adic integers $\chi, \upsilon \in \mathbb{Z}_p^\times$.*

Proof. For some $m \in \mathbb{N}$ and $n \in \mathbb{N}$, $x = p^m\chi$ and $y = p^n\upsilon$, so $\frac{x}{y} = p^{m-n}\frac{\chi}{\upsilon}$. □

Proposition 3.3. *The combined orbit of $\mathbb{Z}$ acting on $\mathbb{Q}_p$ of the elements of the subring $\mathbb{Z}_p^\times \subset \mathbb{Q}_p$ is the entire multiplicative group of the field $\mathbb{Q}_p$.*

Proof. Without loss of generality, let $p^e\frac{x}{y}$ with $x, y \in \mathbb{Z}_p^\times$ and $e \in \mathbb{Z}$ denote an arbitrary element of $\mathbb{Q}_p$. Writing $u = xy^{-1} \in \mathbb{Z}_p^\times$, it is clearly the case that $p^euy = p^ex$. Therefore, $p^e\frac{x}{y} = p^eu$, which is sufficient to prove the proposition. □

Remark 3.4. The exponent e in the decomposition of a p-adic number into the form p^eu for $u \in \mathbb{Z}_p$ defines a valuation on the p-adics [3, p. 12]. Refer to Koblitz [2] for analytic applications of the p-adics which make use of this valuation.

Proposition 3.5. *The multiplicative group $\mathbb{Q}_p^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_p^\times$.*

Proof. By the action of $\mathbb{Z}$ on $\mathbb{Q}_p$, each pair $\left(e, u\right) \in \mathbb{Z}\times\mathbb{Z}_p^\times$ defines a p-adic integer p^eu. Likewise, since each nonzero element of the p-adic field $\mathbb{Q}_p$ can be written as p^eu for some pair $\left(e, u\right) \in \mathbb{Z} \times \mathbb{Z}_p^\times$, each p-adic integer defines a tuple in $\mathbb{Z} \times \mathbb{Z}_p^\times$. Therefore, the map $\varphi : \left(e, u\right) \mapsto p^eu$ is bijective. Moreover, for any pairs $\left(e_1, u\right)$ and $\left(e_2, v\right) \in \mathbb{Z}\times\mathbb{Z}_p^\times$, $\varphi(\left(e_1, u\right)\left(e_2, v\right)) = p^{e_1}up^{e_2}v = \left((p^{e_1} \pmod{p^n})u_n(p^{e_2} \pmod{p^n})v_n\right)_{n\in\mathbb{N}} = \left((p^{e_1} \pmod{p^n})(p^{e_2} \pmod{p^n})u_nv_n\right)_{n\in\mathbb{N}} = \left((p^{e_1+e_2} \pmod{p^n})u_nv_n\right)_{n\in\mathbb{N}} = p^{e_1+e_2}uv = \varphi(\left(e_1 + e_2, uv\right))$. Therefore, since $\varphi : \mathbb{Z}\times\mathbb{Z}_p^\times \to \mathbb{Q}_p$ is a bijective homomorphism, $\mathbb{Z} \times \mathbb{Z}_p^\times \simeq \mathbb{Q}_p$. □

Serre [3] proves further isomorphisms of $\mathbb{Z}_p^\times$ which we quote below without much discussion.

Definition 3.6. Let the component homomorphism $\varepsilon_n : \mathbb{Z}_p^\times \to \mathbb{Z}/p^n\mathbb{Z}$ denote the map given $\left(x_j\right)_{j\in\mathbb{N}} \mapsto x_n$.

Remark 3.7. ε_n defines a homomorphism since for any two $x = \left(x_j\right)_{j\in\mathbb{N}}, y = \left(y_j\right)_{j\in\mathbb{N}} \in \mathbb{Z}_p^\times$, $\varepsilon_n(xy) = \varepsilon_n(\left(x_j y_j\right)_{j\in\mathbb{N}}) = x_n y_n = \varepsilon_n(x)\varepsilon_n(y)$. Note that ε_n is surjective since for any $\bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$, $\varepsilon_n(\left([\bar{a}] \pmod{p^n}\right)_{n\in\mathbb{N}}) = \bar{a}$.

Proposition 3.8. $\mathbb{Z}_p^\times \simeq \ker \varepsilon_1 \times V$ *for some* $V \leq \mathbb{Z}_p^\times$.

Proof. (Sketch) By the Correspondence Theorem, there is a bijection between the subgroups of $\mathbb{Z}_p^\times$ which contain $\ker \varepsilon_1$ and the subgroups of $\mathbb{Z}_p^\times/\ker \varepsilon_1 \simeq \operatorname{im} \varepsilon_1 = \mathbb{Z}/p\mathbb{Z}$. However, since p is prime, the only subgroups of $\mathbb{Z}_p^\times/\ker \varepsilon_1$ are trivial, which means the only subgroups of $\mathbb{Z}_p$ which contain $\ker \varepsilon_1$ are $\{\left(1\right)_{n\in\mathbb{N}}\}$ and $\ker \varepsilon_1$. Note that the set of all units of $\mathbb{Z}_p$ which are not in $\ker \varepsilon_1$ also form a subgroup of $\mathbb{Z}_p$ (asserted without proof). Therefore, $\ker \varepsilon_1 \cap V = \left\{\left(1\right)_{n\in\mathbb{N}}\right\}$ where $V = \mathbb{Z}_p^\times - \ker \varepsilon_1$, and $V(\ker \varepsilon_1) = \mathbb{Z}_p^\times$ as $\ker \varepsilon_1 \cup V = \mathbb{Z}_p^\times$. Both are also normal in $\mathbb{Z}_p^\times$, so $\mathbb{Z}_p^\times \simeq \ker \varepsilon_1 \times V$. □

REFERENCES

[1] KATOK, S. *p-adic Analysis Compared with Real*, vol. 37. American Mathematical Soc., 2007.

[2] KOBLITZ, N. *A course in number theory and cryptography*, vol. 114. Springer Science & Business Media, 1994.

[3] SERRE, J.-P. *A course in arithmetic*. Springer-Verlag, 1973.