p-adic Tools for the Remnant Rings

In R17.1.19 it was shown that for p prime $\mathbf{R}_p$ is topologically isomorphic to the p-adic integers. This was done in a non-constructive manner by using the universal property of inverse limits.

In the first chapter of [1], Robert describes several representations of the p-adic integers (including the projective limit representation, which is closely related to the remnant ring representation) but makes central use of the traditional definition of them as formal power series. With that definition he presents certain basic definitions and results useful in their study. It is the purpose of this section to reformulate some of those tools within the framework of the remnant rings, including the cases of $\mathbf{R}_k$ when k is not a prime.

This reformulation is based on a heuristic, which starts with the following definition and which also suggests constructively a possible map from $\mathbf{R}_p$, p prime, to the formal power series representation of the p-adic integers.

This definition and what follows make extensive use of the sequence associated with a non-point ultrafilter in $\mathbb{N}_k$ as defined in R10.2.3 as well as other facts and terminology from [2], [3], and [4]. Recall that the additive identity in $\mathbf{R}_k$ is $f_k(0)$, which is associated with $\{k^n\}$. By R10.2.4 the sequence associated with a non-point ultrafilter is unique.

Definition R20.1 Let $k \geq 2$ be in $\mathbb{N}$ and let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. Define the derived sequence $\{a_n\}_{n=0}^{\infty}$ determined by $\mathcal{F}$ as follows: If $\mathcal{F} = f_k(0)$, let $a_n = 0$ for all $n \geq 0$. Otherwise, let l be the smallest of $\{n : x_n \neq k^n\}$. If $l = 1$, let $a_0 = x_1$ and $a_n = (x_{n+1} - x_n)/k^n$ for $n \geq 1$. If $l > 1$, let $a_0 = a_1 = \cdots = a_{l-2} = 0$, $a_{l-1} = x_l/k^{l-1}$, and let $a_n = (x_{n+1} - x_n)/k^n$ for $n \geq l$.

The creates some possible confusion because there are now two sequences related to $\mathcal{F} \in \mathbf{R}_k$, $\{x_n\}_{n=1}^{\infty}$ as in R10.2.3 and $\{a_n\}_{n=0}^{\infty}$ as above. An attempt will be made to distinguish them by terminology: $\{x_n\}_{n=1}^{\infty}$ will always be the sequence associated with $\mathcal{F}$ and $\{a_n\}_{n=0}^{\infty}$ the sequence derived from $\mathcal{F}$.

Lemma R20.2 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$. Let $\{a_n\}_{n=0}^{\infty}$ be the sequence derived from $\mathcal{F}$. Then

i) For every $n \geq 0$, $a_n \in \{0, 1, \ldots, k-1\}$.

ii) If $\mathcal{F} = f_k(m)$ for some $m \in \mathbb{N}$, then, for all but finitely many n, $a_n = 0$.

Proof: Assume $\mathcal{F} \neq f_k(0)$ and let $\{x_n\}$ be associated with $\mathcal{F}$. Let l be the smallest of $\{n : x_n \neq k^n\}$. For i) first note that for $n \geq l$, by R10.2.5i $x_{n+1} = x_n + tk^n$ where $t \in \{0, 1, \ldots, k-1\}$. By definition $a_n = t$ and i) holds in this case. If $l = 1$, then $x_1 \neq k$. Since $x_1 \in \{1, 2, \ldots, k-1\}$, $a_0 = x_1 \in \{1, 2, \ldots, k-1\}$. If $l > 1$, then $a_0 = a_1 = \cdots = a_{l-2} = 0$. Finally, $x_{l-1} = k^{l-1}$ and so $x_l = k^{l-1} + tk^{l-1}$ where $t \in \{0, 1, \ldots, k-1\}$. Since $x_l \neq k^l$, $t \leq k-2$ and $a_{l-1} = t+1$ is in $\{1, 2, \ldots, k-1\}$. Thus i) holds. Now assume $\mathcal{F} = f_k(m)$ for some $m \in \mathbb{N}$. By R12.5.9ii and R16.6 $x_n \equiv m \bmod k^n$ for all n and so for all but finitely many n, $x_n = m$. By definition R20.1 $n \geq l$ implies $a_n = (x_{n+1} - x_n)/k^n$. This verifies ii).

Lemma R20.3 Let $k \geq 2$ and $\mathcal{F}$ in $\mathbf{R}_k$ be associated with $\{x_n\}$. Assume $\mathcal{F} \neq f_k(0)$ and let l be the smallest of $\{n : x_n \neq k^n\}$. Then $x_n \neq k^n$ for $n \geq l$.

Proof: By induction on n, $n \geq l$. The statement is true for $n = l$ by the choice of l. Assume $x_n \neq k^n$. Then $1 \leq x_n < k^n$. By R10.2.5i $x_{n+1} = x_n + tk^n$ where $t \in \{0, 1, \ldots, k-1\}$ so that $x_{n+1} < k^n + (k-1)k^n = k^{n+1}$.

Lemma R20.4 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$ with $\mathcal{F} \neq f_k(0)$. Let $\mathcal{F}$ be associated with $\{x_n\}$ and let l be the smallest element of $\{n : x_n \neq k^n\}$. Assume $l > 1$. Then

i) $k^{l-1} |\ x_n$ for every $n \geq l-1$.
ii) $x_n = k^n$ for $1 \leq n \leq l-1$.
iii) k^l does not divide x_n for $n \geq l$.

Proof: Since $l > 1$, $x_{l-1} = k^{l-1}$. For $n \geq l-1$, by R10.2.5ii, $k^{l-1} | (x_n - x_{l-1})$ and part i) follows easily. Part ii) is immediate from the choice of l. For iii), $x_l \in \{1, 2, \ldots, k^l\}$ and $x_l \neq k^l$ imply k^l does not divide x_l. Assume, for some $n \geq l$, k^l does not divide x_n. By R10.2.5i $x_{n+1} = x_n + tk^n$ and, since $k^l |\, k^n$, k^l does not divide x_{n+1}.

Lemma R20.5 Let $k, m \in \mathbb{N}$ with $k \geq 2$. Let $\{a_n\}_{n=0}^{\infty}$ be the sequence derived from $f_k(m)$. Then $m = \Sigma_{n=0}^{\infty} a_n k^n$.

Proof: First note that by R20.2ii all but finitely many terms of the infinite series are zero and so convergence is clear. From elementary number theory there exist an integer $t \geq 0$ and $b_0, b_1, \ldots, b_t$ with $b_t \neq 0$ and each $b_i \in \{0, 1, \ldots, k-1\}$ such that $m = \Sigma_{i=0}^{t} b_i k^i$. For convenience, define $b_i = 0$ for all $i > t$. $f_k(m)$ is associated with $\{x_n\}$, where $x_n \in \{1, 2, \ldots, k^n\}$ and $x_n \equiv m \bmod k^n$ for all $n \geq 1$ so that $x_n \equiv \Sigma_{i=0}^{n-1} b_i k^i \bmod k^n$ for all n. Since $m \geq 1$, let l be the smallest of $\{n : x_n \neq k^n\}$. For $n \geq l$, $x_n \neq k^n$ and so $\Sigma_{i=0}^{n-1} b_i k^i$ cannot be 0. Since both x_n and $\Sigma_{i=0}^{n-1} b_i k^i$ are in $\{1, 2, \ldots, k^n - 1\}$, the congruence must be equality, i.e., $x_n = \Sigma_{i=0}^{n-1} b_i k^i$ for $n \geq l$. In this case $a_n = (x_{n+1} - x_n)/k^n$, i.e., $a_n = b_n$. For $n < l$, there are three cases. If $l = 1$, then $x_1 \neq k$ so that $b_0 \neq 0$ and $x_1 = b_0$. By definition $a_0 = x_1 = b_0$. If $l > 1$ and $n < l-1$, $a_n = 0$ by definition and $x_{n+1} = k^{n+1}$. Since $0 \leq \Sigma_{i=0}^{n} b_i k^i < k^{n+1}$, $b_n = 0$ also. Finally, if $l > 1$ and $n = l-1$, $a_n = x_{n+1}/k^n$. As in the previous case, $b_i = 0$ for $i < n$. Since $x_{n+1} \neq k^{n+1}$, $x_{n+1} = b_n k^n$ so that $a_n = b_n$. To summarize, $a_n = b_n$ for all n so that the conclusion holds.

When p is prime, definition R20.1 determines a map from $\mathbf{R}_p$ to the p-adic integers traditionally defined as a set of formal power series. Because of Lemma R20.5 and R17.1.19, it is conjectured (but not verified) that this map is a homeomorphism, possibly with other useful properties. See also Robert's comment on p. 34 of [1].

Definition R20.1 allows the definition below of rord, which has similar properties to the order function defined by Robert [1 ; p. 4]. In the case of a prime, rord and Robert's order function may be (again, not proven) essentially equivalent.

Lemma R20.6 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$. Let $\{a_n\}_{n=0}^{\infty}$ be the sequence derived from $\mathcal{F}$. Then $a_n = 0$ for every $n \geq 0$ if and only if $\mathcal{F} = f_k(0)$.

Proof: Let $\mathcal{F}$ in $\mathbf{R}_k$ be associated with $\{x_n\}$. If $\mathcal{F} = f_k(0)$, then by definition R20.1 $a_n = 0$ for all $n \geq 0$. If $\mathcal{F} \neq f_k(0)$, by R10.2.4 $x_n \neq k^n$ for some n. Let l be the smallest of $\{n : x_n \neq k^n\}$. If $l = 1$, $x_1 \in \{1, 2, \ldots, k-1\}$ so that $a_0 = x_1 \neq 0$. If $l > 1$, by definition $a_{l-1} = x_l / k^{l-1}$. We also have $x_{l-1} = k^{l-1}$ and so $x_l = k^{l-1} + tk^{l-1}$ where $t \in \{0, 1, \ldots, k-1\}$. Since $x_l \neq k^l$, $t \leq k-2$ and $a_{l-1} = t+1$ is in $\{1, 2, \ldots, k-1\}$, i.e., $a_{l-1} \neq 0$.

Definition R20.7 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$ with $\mathcal{F} \neq f_k(0)$. Let $\{a_n\}_{n=0}^{\infty}$ be the sequence derived from $\mathcal{F}$. rord($\mathcal{F}$) is defined to be the smallest element of $\{n : a_n \neq 0\}$.

Lemma R20.8 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$ with $\mathcal{F} \neq f_k(0)$. Let

$\mathcal{F}$ be associated with $\{x_n\}$ and let l be the smallest element of $\{n : x_n \neq k^n\}$. Then $\text{rord}(\mathcal{F}) = l - 1$.

Proof: If $l = 1$, $x_1 \in \{1, 2, \ldots, k-1\}$ and by definition $a_0 = x_1$. Since $a_0 \neq 0$, $\text{rord}(\mathcal{F}) = 0$. If $l > 1$, by definition R20.1 $a_0 = a_1 = \cdots = a_{l-2} = 0$ and $a_{l-1} = x_l/k^{l-1}$. Then $a_{l-1} \neq 0$ and $\text{rord}(\mathcal{F}) = l - 1$.

The previous lemma shows that the function v defined in R17.1.7 is simply rord+1. In R17.1.12, with k assumed prime, v was shown to be a euclidean valuation for the ring $\mathbf{R}_k$. In the following results there are other connections and overlaps with the first subsection of R17, but they will not be noted in detail.

Proposition R20.9 Let $p \in \mathbb{N}$ with p prime and let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_p$ with $\mathcal{F} \neq f_p(0)$ and $\mathcal{G} \neq f_p(0)$. Then $\text{rord}(\mathcal{FG}) = \text{rord}(\mathcal{F}) + \text{rord}(\mathcal{G})$.

Proof: By R12.5.16 $\mathcal{FG} \neq f_p(0)$ and so $\text{rord}(\mathcal{FG})$ is defined. Let $\mathcal{F}$ be associated with $\{x_n\}$, let $\mathcal{G}$ be associated with $\{y_n\}$, and let $\mathcal{FG}$ be associated with $\{z_n\}$. By R12.4.4 $z_n \equiv x_n y_n \bmod p^n$ for every n. Let $s = \text{rord}(\mathcal{F})$ and $t = \text{rord}(\mathcal{G})$. We proceed by cases. First, assume $s = t = 0$. Then $z_1 = p$ would imply $p \,|\, x_1 y_1$ so that the prime p divides either x_1 or y_1, a contradiction. By R20.8 $\text{rord}(\mathcal{FG}) = 0$. Next suppose $s \neq 0$ and $t = 0$. By lemmas R20.4ii and R20.8, for $1 \leq n \leq s$, $x_n = p^n$ and $p^n \,|\, x_n y_n$ so that $z_n = p^n$ and $\text{rord}(\mathcal{FG}) \geq s$. Also $x_{s+1} < p^{s+1}$ and, since $t = 0$, p does not divide y_{s+1}. Since p is prime, p^{s+1} does not divide $x_{s+1} y_{s+1}$ so that $z_{s+1} < p^{s+1}$ and $\text{rord}(\mathcal{FG}) \leq s$. The case with $s = 0$ and $t \neq 0$ is similar. Lastly, assume $s > 0$ and $t > 0$. By R20.4 and R20.8 $x_n = p^n$ for $1 \leq n \leq s$ and $y_n = p^n$ for $1 \leq n \leq t$. It follows easily that $p^n \,|\, x_n y_n$ and so $z_n = p^n$ for $1 \leq n \leq s + t$. Thus $\text{rord}(\mathcal{FG}) \geq s + t$. If $z_{s+t+1} = p^{s+t+1}$, then, since p is prime, either $p^{s+1} \,|\, x_{s+t+1}$ or $p^{t+1} \,|\, y_{n+t+1}$, which contradicts R20.4iii. Thus $\text{rord}(\mathcal{FG}) = s + t$.

Note that in $\mathbf{R}_6$ $f_6(2) f_6(3) = f_6(6) \neq f_6(0)$ and $\text{rord}(f_6(2)) = \text{rord}(f_6(3)) = 0$ but $\text{rord}(f_6(6)) = 1$, which shows that R20.9 does not directly generalize to non-prime k.

Proposition R20.10 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$ with $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$. Assume $\mathcal{F} + \mathcal{G} \neq f_k(0)$ as well. Then $\text{rord}(\mathcal{F} + \mathcal{G}) \geq \min\{\text{rord}(\mathcal{F}), \text{rord}(\mathcal{G})\}$.

Proof: Let $s = \text{rord}(\mathcal{F})$ and $t = \text{rord}(\mathcal{G})$. Assume both s, t are non-zero since otherwise the conclusion clearly holds. Let $\mathcal{F}$ be associated with $\{x_n\}$, $\mathcal{G}$ with $\{y_n\}$, and $\mathcal{F} + \mathcal{G}$ with $\{z_n\}$. By R20.8 $x_s = k^s$ and $y_t = k^t$. Let $m = \min\{s, t\}$. By R20.4ii $x_m = k^m = y_m$. By R12.4.4 $z_m \equiv x_m + y_m \bmod k^m$, i.e., $z_m \equiv 0 \bmod k^m$. Since $z_m \in \{1, 2, \ldots, k^m\}$, $z_m = k^m$. By R20.4 and R20.8 $\text{rord}(\mathcal{F} + \mathcal{G}) \geq m$.

Proposition R20.11 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$ with $\mathcal{F} \neq f_k(0)$. Suppose $\{\mathcal{F}_j\}$ is a sequence in $\mathbf{R}_k$ with $\{\mathcal{F}_j\}$ converging to $\mathcal{F}$. Then eventually $\mathcal{F}_j \neq f_k(0)$ and $\text{rord}(\mathcal{F}_j) = \text{rord}(\mathcal{F})$.

Proof: Let $\{{}^j x_n\}$ be the sequence associated with $\mathcal{F}_j$ and let $\{x_n\}$ be the sequence associated with $\mathcal{F}$. Let l be the smallest element of $\{n : x_n \neq k^n\}$. By l applications of R17.2.16 there is m such that $j \geq m$ implies ${}^j x_t = x_t$ for $1 \leq t \leq l$. Thus, for $j \geq m$, ${}^j x_l = x_l \neq k^l$. If $l = 1$, the conclusion follows from R20.8. If $l > 1$, then ${}^j x_{l-1} = x_{l-1} = k^{l-1}$ and the conclusion follows from R20.4.ii and R20.8.

Note that $\{f_k(k^n)\}$ converges to $f_k(0)$ in $\mathbf{R}_k$ and $\text{rord}(f_k(k^n)) = n$, while rord is undefined at $f_k(0)$. Because of such examples, it might make sense to follow Robert a bit farther and assign a value of ∞ to rord at $f_k(0)$, but that isn't done here.

Definition R20.12 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$. $|\mathcal{F}|$ is defined to be 0 if

$\mathcal{F} = f_k(0)$ and $1/k^m$, where $m = \text{rord}(\mathcal{F})$, if $\mathcal{F} \neq f_k(0)$.

Proposition R20.13 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$. Then

i) $|\mathcal{F} + \mathcal{G}| \leq \max\{|\mathcal{F}|, |\mathcal{G}|\}$.

ii) $|\mathcal{F} + \mathcal{G}| \leq |\mathcal{F}| + |\mathcal{G}|$.

iii) $|-\mathcal{F}| = |\mathcal{F}|$.

iv) If k is prime, then $|\mathcal{F}\mathcal{G}| = |\mathcal{F}| \cdot |\mathcal{G}|$.

Proof: Since $|\ldots|$ is non-negative by definition, the first conclusion holds if $\mathcal{F} + \mathcal{G} = f_k(0)$. It is also clear if $\mathcal{F} = f_k(0)$ or $\mathcal{G} = f_k(0)$, and so assume $\mathcal{F} + \mathcal{G} \neq f_k(0)$, $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$. Let $m = \text{rord}(\mathcal{F} + \mathcal{G})$, $r = \text{rord}(\mathcal{F})$, and $s = \text{rord}(\mathcal{G})$. If $r \leq s$, then $k^r \leq k^s$ so that $\max\{|\mathcal{F}|, |\mathcal{G}|\} = 1/k^r$. By R20.10 $m \geq r$ so that $k^m \geq k^r$ and i) holds. If $s \leq r$, i) follows similarly. Conclusion ii) follows since $\max\{|\mathcal{F}|, |\mathcal{G}|\} \leq |\mathcal{F}| + |\mathcal{G}|$. Part iii) clearly holds if $\mathcal{F} = f_k(0)$ and so assume $\mathcal{F} \neq f_k(0)$. Let $\mathcal{F}$ be associated with $\{x_n\}$ and let $-\mathcal{F}$ be associated with $\{y_n\}$. By R12.6.2 $y_n \equiv k^n - x_n \bmod k^n$. Since x_n and y_n are chosen from $\{1, 2, \ldots, k^n\}$, $y_n = k^n$ if and only if $x_n = k^n$. By R20.8 $\text{rord}(\mathcal{F}) = \text{rord}(-\mathcal{F})$ and iii) follows. Finally part iv) is clear if $\mathcal{F} = f_k(0)$ or $\mathcal{G} = f_k(0)$, and so assume $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$. Let $r = \text{rord}(\mathcal{F})$ and $s = \text{rord}(\mathcal{G})$. By R20.9 $\text{rord}(\mathcal{F}\mathcal{G}) = r + s$ and so $|\mathcal{F}\mathcal{G}| = 1/p^{r+s} = 1/p^r \cdot 1/p^s = |\mathcal{F}| \cdot |\mathcal{G}|$.

Proposition R20.14 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \neq f_k(0)$ be in $\mathbf{R}_k$. Suppose $\{\mathcal{F}_n\}$ is a sequence in $\mathbf{R}_k$ with $\{\mathcal{F}_n\}$ converging to $\mathcal{F}$. Then eventually $|\mathcal{F}_n| = |\mathcal{F}|$.

Proof: This is immediate from R20.11 and definition R20.12.

Note that the example following R20.11 shows that $|\ldots|$ need not map a sequence converging to $f_k(0)$ to an eventually constant sequence, but the following does hold.

Proposition R20.15 Let $k \in \mathbb{N}$ with $k \geq 2$. Suppose $\{\mathcal{F}_n\}$ is a sequence in $\mathbf{R}_k$ with $\{\mathcal{F}_n\}$ converging to $f_k(0)$. Then $|\mathcal{F}_n|$ converges to 0 with the usual topology on the reals.

Proof: Let $\{{}^j x_n\}$ be the sequence associated with $\mathcal{F}_j$. Of course, $\{k^n\}$ is the sequence associated with $f_k(0)$. For $\epsilon > 0$ pick m such that $1/k^m < \epsilon$. By R17.2.16 there is N such that $j \geq N$ implies ${}^j x_m = k^m$. By R20.8 and R20.4ii $j \geq N$ implies $\text{rord}(\mathcal{F}_j) \geq m$ so that $|\mathcal{F}_j| \leq 1/k^m < \epsilon$.

Proposition R20.16 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$. Then

i) If $\mathcal{F}$ is invertible, then $|\mathcal{F}| = 1$.

ii) If k is prime, then $\mathcal{F}$ is invertible if and only if $|\mathcal{F}| = 1$.

Proof: Let $\{x_n\}$ be the sequence associated with $\mathcal{F}$. By R17.1.2 $\mathcal{F}$ is invertible if and only if x_1 is invertible mod k. If $\mathcal{F}$ is invertible, $x_1 \neq k$ so that $\text{rord}(\mathcal{F}) = 0$ and by definition $|\mathcal{F}| = 1$. For ii) assume k is prime and $|\mathcal{F}| = 1$. Clearly $\text{rord}(\mathcal{F}) = 0$ so that $x_1 \neq k$. Thus $x_1 \in \{1, 2, \ldots, k-1\}$ and, since k is prime, x_1 is invertible mod k.

In $\mathbf{R}_6$ observe that $f_6(2)$ is not invertible by R17.1.2 but $|f_6(2)| = 1$. This example shows that the converse of R20.16i is false in the non-prime case.

A version of the next lemma, with the added assumption that $\mathcal{F} \neq f_k(0)$, is an easy corollary of R20.16ii and R20.11 in the case of k prime.

Lemma R20.17 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$. Suppose $\{\mathcal{F}_j\}$ is a sequence in $\mathbf{R}_k$ with $\{\mathcal{F}_j\}$ converging to $\mathcal{F}$. Then the following are equivalent:

i) $\mathcal{F}$ is invertible.

ii) $\{\mathcal{F}_j\}$ is eventually invertible.

iii) $\{\mathcal{F}_j\}$ is frequently invertible.

Proof: Let $\{{}^j x_n\}$ be the sequence associated with $\mathcal{F}_j$ and let $\{x_n\}$ be the sequence associated with $\mathcal{F}$. By R17.2.16 there is m such that $j \geq m$ implies ${}^j x_1 = x_1$. If $\mathcal{F}$ is invertible, by R17.1.2 $\mathcal{F}_j$ is eventually invertible. Obviously ii) implies iii). Finally assume iii). Pick $j \geq m$ such that $\mathcal{F}_j$ is invertible. By R17.1.2 $x_1 = {}^j x_1$ is invertible mod k and so $\mathcal{F}$ is invertible.

Corollary R20.18 Let $k \in \mathbb{N}$ with $k \geq 2$. Then the set of invertible elements in $\mathbf{R}_k$ is clopen.

Proof: In any compact topological ring with unity, the set of invertible elements is closed. (That also follows immediately from R20.17 for $\mathbf{R}_k$.) Now let $\{\mathcal{F}_n\}$ be a sequence of non-invertible elements in $\mathbf{R}_k$ with $\{\mathcal{F}_n\}$ converging to $\mathcal{F}$. By R20.17 $\mathcal{F}$ must be non-invertible and so the set of non-invertible elements is closed. Its complement, the set of invertible elements, must be open.

Definition R20.19 Let $k \in \mathbb{N}$ with $k \geq 2$. Define d_k by $d_k(\mathcal{F}, \mathcal{G}) = |\mathcal{F} - \mathcal{G}|$, where $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$.

The next lemma mentions the ultrametric property, which is defined for a metric ρ by $\rho(x, y) \leq \max\{\rho(x, z), \rho(y, z)\}$ for any x, y, z. In the first section of chapter 2 in [1], Robert develops some of the unusual properties of ultrametrics, e.g., any point of a ball can serve as its center and a sequence $\{x_n\}$ is Cauchy if and only if $\rho(x_n, x_{n+1}) \to 0$.

Lemma R20.20 Let $k \in \mathbb{N}$ with $k \geq 2$. Then

i) d_k is a metric on $\mathbf{R}_k$.

ii) d_k is invariant with respect to addition in $\mathbf{R}_k$.

iii) d_k has the ultrametric property.

Proof: It is clear from R20.12 that d_k is non-negative and $d_k(\mathcal{F}, \mathcal{G}) = 0$ if and only if $\mathcal{F} = \mathcal{G}$. Symmetry follows from R20.13iii and the triangle inequality from R20.13ii. Thus part i) holds. Now let $\mathcal{F}, \mathcal{G}, \mathcal{H} \in \mathbf{R}_k$. By definition $d_k(\mathcal{F}+\mathcal{H}, \mathcal{G}+\mathcal{H}) = |(\mathcal{F}+\mathcal{H})-(\mathcal{G}+\mathcal{H})| = |\mathcal{F}-\mathcal{G}| = d_k(\mathcal{F}, \mathcal{G})$ and so ii) holds. For iii) $d_k(\mathcal{F}, \mathcal{G}) = |\mathcal{F}-\mathcal{G}| = |(\mathcal{F}-\mathcal{H})+(\mathcal{H}-\mathcal{G})|$ and so by R20.13i $d_k(\mathcal{F}, \mathcal{G}) \leq \max\{d_k(\mathcal{F}, \mathcal{H}), d_k(\mathcal{G}, \mathcal{H})\}$ as required for the ultrametric property.

The next few results use a notation introduced in [2]: For $j, k \in \mathbb{N}$ with $k \geq 2$ and $t \in \{1, 2, \ldots, k^j\}$, $C_j^t(k)$ is the equivalence class in $\mathbb{N}$ of t mod k^j.

Lemma R20.21 Let $j, k \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. Let $t \in \{1, 2, \ldots, k^j\}$. Then $C_j^t(k) \in \mathcal{F}$ if and only if $x_j = t$.

Proof: $C_j^t(k)$ is in $\mathcal{Z}(E_j(k))$ and is associated with $\{1, 2, \ldots, k^j\} - \{t\}$. By definition R10.2.3 $\mathcal{F} \cap \mathcal{Z}(E_j(k)) = \{Z \in \mathcal{Z}(E_j(k)) : Z \text{ is associated with } \Delta \subseteq \{1, 2, \ldots, k^j\} - \{x_j\}\}$. The conclusion follows immediately.

Lemma R20.22 Let $k \in \mathbb{N}$ with $k \geq 2$. Then $\{Z^\omega : Z \in \mathcal{Z}_k\}$ is a clopen basis for $\mathbb{N}_k$.

Proof: As noted in P3.6 this set is a closed basis and so the collection of complements is an open basis. By R9.1.7 and definition R10.1.3, $\mathcal{Z}_k$ is closed under complementation. It is easy to check that the complement of the closed $(\mathbb{N} - Z)^\omega$ is Z^ω and the conclusion follows.

Proposition R20.23 Let $k \in \mathbb{N}$ with $k \geq 2$. Then

i) The topology generated by d_k is the compactification topology of $\mathbf{R}_k$.

ii) Every ϵ-ball generated by d_k is clopen.

Proof: Let τ denote the topology on $\mathbf{R}_k$ as a subspace of $\mathbb{N}_k$ and let $\tau(d_k)$ denote the

topology generated by d_k. Since $\tau(d_k)$ is Hausdorff and τ is compact, for i) it is sufficient to show that $\tau(d_k) \subseteq \tau$. Let $\epsilon > 0$. Let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. Since $d_k \leq 1$ by definition, for $\epsilon > 1$, $B(\mathcal{F}, \epsilon) = \mathbf{R}_k$ and so assume $\epsilon \leq 1$. Let j be the unique natural number such that $1/k^j < \epsilon \leq 1/k^{j-1}$. Let $Z = C_j^t(k)$ where $t = x_j$. By R20.21 $\mathcal{F} \in Z^\omega$. It will be shown that $B(\mathcal{F}, \epsilon) = Z^\omega \cap \mathbf{R}_k$. First let $\mathcal{G} \neq \mathcal{F}$ be in $B(\mathcal{F}, \epsilon)$. Let $\mathcal{G}$ be associated with $\{y_n\}$ and $\mathcal{F} - \mathcal{G}$ with $\{z_n\}$. Since $0 < |\mathcal{F} - \mathcal{G}| < 1/k^{j-1}$, $|\mathcal{F} - \mathcal{G}| = 1/k^m$ where $m \geq j$. By R20.8 and R20.4ii $z_n = k^n$ for all $n \leq m$. In particular, $z_j = k^j$. Since $z_j \equiv x_j - y_j \bmod k^j$ and $x_j, y_j \in \{1, 2, \ldots, k^j\}$, $y_j = x_j = t$ so that $\mathcal{G} \in Z^\omega \cap \mathbf{R}_k$ by R20.21. Next let $\mathcal{G} \in Z^\omega \cap \mathbf{R}_k$ be associated with $\{y_n\}$. By R20.21 $x_j = y_j$ and so again letting $\mathcal{F} - \mathcal{G}$ be associated with $\{z_n\}$ and assuming $\mathcal{F} \neq \mathcal{G}$, $z_j = k^j$ and $\operatorname{rord}(\mathcal{F} - \mathcal{G}) \geq j$. Thus $d_k(\mathcal{F}, \mathcal{G}) \leq 1/k^j < \epsilon$ as required. Finally, part ii) follows immediately from the above argument and R20.22.

Proposition R20.24 Let $p \in \mathbb{N}$ be a prime. Let $\mathcal{F}, \mathcal{G}, \mathcal{H} \in \mathbf{R}_p$. Then

i) $d_p(\mathcal{FH}, \mathcal{GH}) = |\mathcal{H}| \cdot d_p(\mathcal{F}, \mathcal{G})$.

ii) $d_p(f_p(p) \cdot \mathcal{F}, f_p(p) \cdot \mathcal{G}) = (1/p) \cdot d_p(\mathcal{F}, \mathcal{G})$.

iii) If $\mathcal{H}$ is invertible, then d_p is invariant under multiplication by $\mathcal{H}$.

Proof: Part i) is clear if $\mathcal{F} = \mathcal{G}$ or $\mathcal{H} = f_p(0)$. In the remaining case let $r = \operatorname{rord}(\mathcal{F} - \mathcal{G})$ and $s = \operatorname{rord}(\mathcal{H})$. By R20.9 $\operatorname{rord}(\mathcal{FH} - \mathcal{GH}) = r + s$ and so $d_p(\mathcal{FH}, \mathcal{GH}) = 1/p^{r+s} = 1/p^s \cdot 1/p^r = |\mathcal{H}| \cdot d_p(\mathcal{F}, \mathcal{G})$. For ii) note that $f_p(p)$ is associated with $\{x_n\}$ where $x_n = p$ for all n. By R20.8 $\operatorname{rord}(f_p(p)) = 1$. By definition R20.12 $|f_p(p)| = 1/p$ and so ii) follows from part i). If $\mathcal{H}$ is invertible, by R20.16i $|\mathcal{H}| = 1$ and so $d_p(\mathcal{FH}, \mathcal{GH}) = d_p(\mathcal{F}, \mathcal{G})$ by i), i.e., iii) holds.

The rest of this section contains results centering on what Robert [0; pp. 45-54] describes as Hensel's Philosophy. This refers to Kurt Hensel, the original discoverer of the p-adic integers.

Given a ring A and a polynomial $P \in A[X_1, X_2, \ldots, X_j]$, $P = 0$ admits a solution in A means there are $a_1, a_2, \ldots, a_j$ in A such that $P(a_1, a_2, \ldots, a_j) = 0$. In what follows a polynomial in $\mathbf{Z}[X_1, X_2, \ldots, X_j]$ will be treated as polynomial with coefficients in $\mathbf{Z} / < k^t >$, respectively $\mathbf{R}_k$ or $\mathbf{R}_\infty$, by identifying each integer coefficient z with $z+ < k^t >$, respectively $f_k(z)$ or $f_\infty(z)$.

As a first step, a slightly generalized version of R17.1.17 will be needed.

Lemma R20.25 Let $k \in \mathbb{N}$ with $k \geq 2$. For $i \in \mathbb{N}$, let $\pi_i : \mathbf{R}_k \to \mathbf{Z} / < k^i >$ by $\pi_i(\mathcal{F}) = x_i + < k^i >$, where $\mathcal{F}$ is associated with $\{x_n\}$. Then

i) For every $t \in \mathbf{Z}$, $\pi_i(f_k(t)) = t + < k^i >$.

ii) π_i ia a surjective ring homomorphism.

iii) π_i is continuous with the discrete topology on the image space.

Proof: For i) recall that $f_k(t)$ is associated with $\{x_n\}$, where $x_n \equiv t \bmod k^n$, so that $x_i + < k^i >= t + < k^i >$. Part ii) follows easily from i) and R12.4.4. For iii) let $t \in \{1, 2, \ldots, k^i\}$. $C_i^t(k) \in \mathcal{Z}_k$ and by R20.22 $(C_i^t(k))^\omega \cap \mathbf{R}_k$ is clopen in $\mathbf{R}_k$. R20.21 makes it is easy to check $\pi_i^{-1}[\{t + < k^i >\}] = (C_i^t(k))^\omega \cap \mathbf{R}_k$, which shows continuity.

Lemma R20.26 Let $j, k \in \mathbb{N}$ with $k \geq 2$, let $P \in \mathbf{Z}[X_1, X_2, \ldots, X_j]$, and let $b_1, b_2, \ldots, b_j \in \mathbf{Z}$. Assume $c = P(b_1, b_2, \ldots, b_j)$. Then $P(f_k(b_1), f_k(b_2), \ldots, f_k(b_j)) = f_k(c)$.

Proof: Write P as $\Sigma_{d \in \Delta} c_d X_1^{n(1,d)} X_2^{n(2,d)} \ldots X_j^{n(j,d)}$, where Δ is a finite set, each

$c_d \in \mathbf{Z}$, and each $n(i,d)$ a non-negative integer. With the identification mentioned above,

$$P(f_k(b_1), f_k(b_2), \ldots, f_k(b_j)) = \Sigma_{d\in\Delta} f_k(c_d) f_k(b_1)^{n(1,d)} f_k(b_2)^{n(2,d)} \ldots f_k(b_j)^{n(j,d)}$$

By R16.3 and R16.6 f_k is a ring homomorphism and so

$$P(f_k(b_1), f_k(b_2), \ldots, f_k(b_j)) = f_k(\Sigma_{d\in\Delta} c_d b_1^{n(1,d)} b_2^{n(2,d)} \ldots b_j^{n(j,d)})$$

Thus the conclusion holds.

The next proposition is a version of what Robert calls the first principle of Hensel's Philosophy. This proposition can be easily extended to sets of polynomials, with a corollary for algebraic varieties.

Proposition R20.27 Let $j, k \in \mathbb{N}$ with $k \geq 2$ and let $P \in \mathbf{Z}\ [X_1, X_2, \ldots, X_j]$. The following are equivalent:

i) $P = 0$ admits a solution in $\mathbf{R}_k$.

ii) For every $t \in \mathbb{N}$, $P = 0$ admits a solution in $\mathbf{Z} / < k^t >$.

iii) For each $t \in \mathbb{N}$, $P(a_1^t, a_2^t, \ldots, a_j^t) \equiv 0 \bmod k^t$ for some $a_1^t, a_2^t, \ldots, a_j^t$ in $\mathbf{Z}$.

Proof: Assume i) with $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j) = f_k(0)$, the additive identity in $\mathbf{R}_k$. Let $t \in \mathbb{N}$ and let π_t be defined as in R20.25. By R20.25i and R20.25ii $\pi_t(P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)) = P(\pi_t(\mathcal{F}_1), \pi_t(\mathcal{F}_2), \ldots, \pi_t(\mathcal{F}_j)) = \pi_t(f_k(0)) = 0 + < k^t >$, the additive identity in $\mathbf{Z} / < k^t >$. Thus ii) holds. It is clear that ii) implies iii). Lastly assume iii) holds so that there is a sequence of j-tuples, $\{(a_1^t, a_2^t, \ldots, a_j^t)\}$ such that, for each $t \in \mathbb{N}$, $P(a_1^t, a_2^t, \ldots, a_j^t) \equiv 0 \bmod k^t$. The corresponding sequence $\{(f_k(a_1^t), f_k(a_2^t), \ldots, f_k(a_j^t))\}$ in the sequentially compact $\Pi_{i=1}^j \mathbf{R}_k$ has a subsequence convergent to some $(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)$. Let $\phi : \mathbb{N} \to \mathbb{N}$ be an increasing map such that $\{f_k(a_1^{\phi(t)}), f_k(a_2^{\phi(t)}), \ldots, f_k(a_j^{\phi(t)}))\}$ converges to $(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)$. Since addition and multiplication in $\mathbf{R}_k$ are continuous (R12.2.5), P induces a continuous map on $\Pi_{i=1}^j \mathbf{R}_k$ so that $\{P(f_k(a_1^{\phi(t)}), f_k(a_2^{\phi(t)}), \ldots, f_k(a_j^{\phi(t)}))\}$ converges to $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)$. Let $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)$ be associated with $\{y_n\}$ and let $\{P(f_k(a_1^{\phi(t)}), f_k(a_2^{\phi(t)}), \ldots, f_k(a_j^{\phi(t)}))\}$ be associated with $\{{}^{\phi(t)}x_n\}$. Fix $m \in \mathbb{N}$. By R17.2.16 there is l such that $t \geq l$ implies ${}^{\phi(t)}x_m = y_m$. Pick $t \geq l$ with $\phi(t) \geq m$ and let $c_{\phi(t)} = P(a_1^{\phi(t)}, a_2^{\phi(t)}, \ldots, a_j^{\phi(t)})$. If $c_{\phi(t)} = 0$, ${}^{\phi(t)}x_n = k^n$ for all n. If $c_{\phi(t)} \neq 0$, then $c_{\phi(t)} \equiv 0 \bmod k^{\phi(t)}$ by hypothesis, and so by R20.26 ${}^{\phi(t)}x_{\phi(t)} \equiv c_{\phi(t)} \bmod k^{\phi(t)}$. By the definition of the associated sequence ${}^{\phi(t)}x_{\phi(t)} = k^{\phi(t)}$ and by R20.4ii ${}^{\phi(t)}x_m = k^m$. In either case, $y_m = k^m$. Thus $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j) = f_k(0)$ and i) holds.

The next few results show yet again ways in which the composite remnant rings, i.e., $\mathbf{R}_k$ when k is a non-prime and $\mathbf{R}_\infty$, are determined by the p-adic integers.

Corollary R20.28 Let $k, l \in \mathbb{N}$ with $k, l \geq 2$ and $k|l$. Let $P \in \mathbf{Z}\ [X_1, X_2, \ldots, X_j]$. If $P = 0$ admits a solution in $\mathbf{R}_l$, then $P = 0$ admits a solution in $\mathbf{R}_k$.

Proof: By hypothesis and R20.27iii for each $t \in \mathbb{N}$, $P(a_1^t, a_2^t, \ldots, a_j^t) \equiv 0 \bmod l^t$ for some $a_1^t, a_2^t, \ldots, a_j^t$ in $\mathbf{Z}$. Then for each $t \in \mathbb{N}$, $P(a_1^t, a_2^t, \ldots, a_j^t) \equiv 0 \bmod k^t$ for some $a_1^t, a_2^t, \ldots, a_j^t$ in $\mathbf{Z}$, since $k|l$. Another application of R20.27 shows that $P = 0$ admits a solution in $\mathbf{R}_k$.

The next two lemmas are implicit in the second subsection of R17. Their proofs can be facilitated by revisiting some cumbersome notation. Given $a, b \in \mathbb{N}$ with $a, b \geq 2$ and a

dividing b, ${}_ah_b : \mathbf{R}_b \to \mathbf{R}_a$ was defined (17.2.4) by ${}_ah_b(\mathcal{F}) = \mathcal{F} \cap \mathcal{Z}_a$. Next, given $k \in \mathbb{N}$ with $k \geq 2$, let $p_1, p_2, \ldots, p_t$ be all the distinct primes dividing k. $H_k : \mathbf{R}_k \to \Pi_{i=1}^t \mathbf{R}_{p_i}$ was defined (R17.2.18) by $H_k(\mathcal{F}) = ({}_{p_1}h_k(\mathcal{F}), \ldots, {}_{p_t}h_k(\mathcal{F}))$.

Lemma R20.29 Let $k \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G}$ be in $\mathbf{R}_k$. Assume that, for every prime p such that $p|k$, $\mathcal{F} \cap \mathcal{Z}_p = \mathcal{G} \cap \mathcal{Z}_p$. Then $\mathcal{F} = \mathcal{G}$.

Proof: In R17.2.19 H_k as described above was shown to be one-to-one. The definition of H_k and the hypothesis imply $H_k(\mathcal{F}) = H_k(\mathcal{G})$. Thus $\mathcal{F} = \mathcal{G}$.

Lemma R20.30 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $p_1, p_2, \ldots, p_t$ be all the distinct primes dividing k. Assume $\mathcal{F}_i \in \mathbf{R}_{p_i}$ for $i \in \{1, 2, \ldots, t\}$. Then there is a unique $\mathcal{F}$ in $\mathbf{R}_k$ such that $\mathcal{F} \cap \mathcal{Z}_{p_i} = \mathcal{F}_i$ for all i.

Proof: By R20.29 there is at most one such $\mathcal{F}$. By R17.2.19 H_k is onto $\Pi_{i=1}^t \mathbf{R}_{p_i}$ and so there is at least one such $\mathcal{F}$.

Proposition R20.31 Let $k \in \mathbb{N}$ with $k \geq 2$ and let $P \in \mathbf{Z}\ [X_1, X_2, \ldots, X_j]$. Then $P = 0$ admits a solution in $\mathbf{R}_k$ if and only if for every prime p dividing k, $P = 0$ admits a solution in $\mathbf{R}_p$.

Proof: If $P = 0$ admits a solution in $\mathbf{R}_k$, the conclusion is immediate from R20.28. If for every prime p dividing k, $P = 0$ admits a solution in $\mathbf{R}_p$, let $p_1, p_2, \ldots, p_t$ be all the distinct primes dividing k. For $1 \leq i \leq t$ there exist ${}^i\mathcal{F}_1, {}^i\mathcal{F}_2, \ldots, {}^i\mathcal{F}_j$ in $\mathbf{R}_{p_i}$ such that $P({}^i\mathcal{F}_1, \ldots, {}^i\mathcal{F}_j) = f_{p_i}(0)$. By R20.30 and definition R17.2.4 there exist $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j$ in $\mathbf{R}_k$ such that ${}_{p_i}h_k(\mathcal{F}_m) = {}^i\mathcal{F}_m$ for $1 \leq i \leq t$ and $1 \leq m \leq j$. By R17.2.5 each ${}_{p_i}h_k$ is a homomorphism with ${}_{p_i}h_k(f_k(z)) = f_{p_i}(z)$ for all $z \in \mathbf{Z}$ so that ${}_{p_i}h_k(P(\mathcal{F}_1, \ldots, \mathcal{F}_j)) = P({}^i\mathcal{F}_1, \ldots, {}^i\mathcal{F}_j) = f_{p_i}(0)$. Thus $H_k(P(\mathcal{F}_1, \ldots, \mathcal{F}_j)) = (f_{p_1}(0), \ldots, f_{p_j}(0)) = H_k(f_k(0))$. Since H_k is one-to-one, $P(\mathcal{F}_1, \ldots, \mathcal{F}_j) = f_k(0)$ and the desired conclusion holds.

Proposition R20.32 Let $P \in \mathbf{Z}\ [X_1, X_2, \ldots, X_j]$. Then $P = 0$ admits a solution in $\mathbf{R}_\infty$ if and only if $P = 0$ admits a solution in $\mathbf{R}_p$ for every prime p.

Proof: Recall definition R16.17: $\rho_p : \mathbf{R}_\infty \to \mathbf{R}_p$ is defined by $\rho_p(\mathcal{F}) = \mathcal{F} \cap \mathcal{Z}_p$. In R16.18 and R17.3.1 ρ_p was shown to be a continuous ring homomorphism for each p. By R16.19 $\rho_p(f_\infty(z)) = f_p(z)$. As a result, for any $\mathcal{F}_1, \ldots, \mathcal{F}_j$ in $\mathbf{R}_\infty$ and for any prime p, $\rho_p(P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)) = P(\rho_p(\mathcal{F}_1), \ldots, \rho_p(\mathcal{F}_j))$. Now assume $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j) = f_\infty(0)$. Then, for any prime p, $P(\rho_p(\mathcal{F}_1), \ldots, \rho_p(\mathcal{F}_j)) = \rho_p(f_\infty(0)) = f_p(0)$, i.e., $P = 0$ admits a solution in $\mathbf{R}_p$. For the converse select ${}^p\mathcal{F}_1, \ldots, {}^p\mathcal{F}_j$ in $\mathbf{R}_p$ for each prime p such that $P({}^p\mathcal{F}_1, \ldots, {}^p\mathcal{F}_j) = f_p(0)$. By R17.3.16 there exist $\mathcal{F}_1, \ldots, \mathcal{F}_j$ in $\mathbf{R}_\infty$ such that $\rho_p(\mathcal{F}_i) = {}^p\mathcal{F}_i$ for each prime p and $1 \leq i \leq j$. For each prime p, $\rho_p(P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j)) = P({}^p\mathcal{F}_1, \ldots, {}^p\mathcal{F}_j) = f_p(0) = \rho_p(f_\infty(0))$. By R17.3.15 $P(\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_j) = f_\infty(0)$ as required.

To continue with Robert's illustration of Henzel's Philosophy, it is necessary to describe the extension of equivalence mod k^n for the remnant rings. If one uses the formal power series representation of the p-adic integers, this concept is so natural that it hardly needs definition. It is less obvious in the remnant ring representation but still easily described.

Definition R20.33 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_p$ with derived sequences (as in R20.1) $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$. $\mathcal{F} \equiv \mathcal{G} \mod k^t$ if and only if $\Sigma_{i=0}^{t-1} a_i k^i \equiv \Sigma_{i=0}^{t-1} b_i k^i \mod k^t$ in $\mathbf{Z}$.

The next few lemmas show that this is in fact an extension and thus justify using the

same notation for this relation in both $\mathbf{Z}$ and $\mathbf{R}_k$.

Lemma R20.34 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$ with derived sequences (as in R20.1) $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$. If $\mathcal{F} \equiv \mathcal{G} \bmod k^t$, then $a_i = b_i$ for $i \in \{0, 1, \ldots, t-1\}$.

Proof: By R20.2i $a_i, b_i \in \{0, 1, \ldots, k-1\}$ and so by elementary algebra $\Sigma_{i=0}^{t-1} a_i k^i$ and $\Sigma_{i=0}^{t-1} b_i k^i$ are in $\{0, 1, \ldots, k^t - 1\}$. In that range congruence mod k^t implies equality. The uniqueness of the base k representation of a non-negative integer implies $a_i = b_i$ for $i \in \{0, 1, \ldots, t-1\}$.

Lemma R20.35 Let $k, t \in \mathbb{N}$ with $k \geq 2$ and let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$. If $\mathcal{F} \equiv \mathcal{G} \bmod k^t$, then $\mathcal{F} \equiv \mathcal{G} \bmod k^n$ for all $n \leq t$.

Proof: Let $\mathcal{F}, \mathcal{G}$ have derived sequences $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$. By R20.34 $a_i = b_i$ for $i \in \{0, 1, \ldots, t-1\}$ and so $\Sigma_{i=0}^{n-1} a_i k^i = \Sigma_{i=0}^{n-1} b_i k^i$ for any $n \leq t$. By definition $\mathcal{F} \equiv \mathcal{G} \bmod k^n$ for all $n \leq t$.

Lemma R20.36 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_p$ with associated sequences (as in R10.2.3) $\{x_n\}_{n=1}^{\infty}$ and $\{y_n\}_{n=1}^{\infty}$. Assume $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$ with $\mathcal{F} \equiv \mathcal{G} \bmod k^t$. Let l be the smallest element of $\{n : x_n \neq k^n\}$, and m the smallest element of $\{n : y_n \neq k^n\}$. If $l \leq t$ and $m \leq t$, then $l = m$.

Proof: Let $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$ be the derived sequences from $\mathcal{F}, \mathcal{G}$ respectively. By R20.34 $a_i = b_i$ for $i \in \{0, 1, \ldots, t-1\}$. Since $l \leq t$, $b_{l-1} = a_{l-1} = x_l / k^{l-1} \neq 0$. If $m - 1 > l - 1$, $b_{l-1} = 0$ by definition. Thus $m - 1 \leq l - 1$. Similarly $l - 1 \leq m - 1$.

Proposition R20.37 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$ with associated sequences (as in R10.2.3) $\{x_n\}_{n=1}^{\infty}$ and $\{y_n\}_{n=1}^{\infty}$. Then $\mathcal{F} \equiv \mathcal{G} \bmod k^t$ if and only if $x_t = y_t$.

Proof: Let $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$ be the derived sequences from $\mathcal{F}, \mathcal{G}$ respectively. First assume $x_t = y_t$. By R12.5.15 $x_i = y_i$ for $1 \leq i \leq t$. If $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$, by definition R20.1, for $0 \leq i \leq t-1$, $a_i = b_i$. If $\mathcal{F} = f_k(0)$ and $\mathcal{G} \neq f_k(0)$, then $y_i = k^i$ for $1 \leq i \leq t$ and so $b_i = 0 = a_i$ for $0 \leq i \leq t-1$, which holds similarly if $\mathcal{G} = f_k(0)$ and $\mathcal{F} \neq f_k(0)$ and which obviously holds if $\mathcal{F} = \mathcal{G} = f_k(0)$. Then in all cases $\Sigma_{i=0}^{t-1} a_i k^i = \Sigma_{i=0}^{t-1} b_i k^i$ and so the desired congruence follows. Now assume $\mathcal{F} \equiv \mathcal{G} \bmod k^t$. By R20.34 $a_i = b_i$ for $i \in \{0, 1, \ldots, t-1\}$. If $\mathcal{F} = f_k(0) = \mathcal{G}$, then $x_t = k^t = y_t$. If $\mathcal{F} = f_k(0)$ and $\mathcal{G} \neq f_k(0)$, let m be the smallest element of $\{n : y_n \neq k^n\}$. By definition $a_i = 0$ for all i and so $b_i = 0$ for $0 \leq i \leq t-1$. Since $y_n \neq 0$ for all n, by definition R20.1 $b_{m-1} \neq 0$ and so $m - 1 \geq t$. Thus $y_t = k^t = x_t$. Similarly, if $\mathcal{G} = f_k(0)$ and $\mathcal{F} \neq f_k(0)$, $x_t = k^t = y_t$. Lastly suppose $\mathcal{F} \neq f_k(0)$ and $\mathcal{G} \neq f_k(0)$. Let l be the smallest element of $\{n : x_n \neq k^n\}$ and m the smallest element of $\{n : y_n \neq k^n\}$. If $l \geq t + 1$, then, since $b_{m-1} \neq 0$, we also have $m \geq t+1$. Similarly $m \geq t+1$ implies $l \geq t+1$. With both greater than t, $x_t = k^t = y_t$. The remaining case has both l and m less than or equal to t. In this case by R20.36 $l = m$. By definition $x_l / k^{l-1} = a_{l-1} = b_{l-1} = y_l / k^{l-1}$ and so $x_l = y_l$. If $l < t$, $(x_{l+1} - x_l)/k^l = a_l = b_l = (y_{l+1} - y_l)/k^l$ and so $x_{l+1} = y_{l+1}$. Continuing this way until t is reached, one has $x_t = y_t$.

Corollary R20.38 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Equivalence mod k^t is an equivalence relation on $\mathbf{R}_k$.

Proof: Immediate from R20.37.

The next corollary shows that equivalence mod k^t in $\mathbf{R}_k$ extends equivalence mod k^t in $\mathbf{Z}$ and justifies using the same notation for both relations.

Corollary R20.39 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $w, z \in \mathbf{Z}$. Then $w \equiv z \bmod k^t$ in $\mathbf{Z}$ if and only if $f_k(w) \equiv f_k(z) \bmod k^t$ in $\mathbf{R}_k$.

Proof: Let $f_k(z)$ and $f_k(w)$ be associated with $\{x_n\}$ and $\{y_n\}$ respectively. By R16.1 and R16.6 $x_t \equiv z \bmod k^t$ and $y_t \equiv w \bmod k^t$. If $w \equiv z \bmod k^t$, then $y_t \equiv x_t \bmod k^t$. By R10.2.3 $x_y, y_t \in \{1, 2, \ldots, k^t\}$ and so $y_t = x_t$. By R20.37 $f_k(w) \equiv f_k(z) \bmod k^t$ in $\mathbf{R}_k$. Conversely, if $f_k(w) \equiv f_k(z) \bmod k^t$ in $\mathbf{R}_k$, by R20.37 $y_t = x_t$ and so $w \equiv z \bmod k^t$ in $\mathbf{Z}$.

Corollary R20.40 Let $k \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F} \in \mathbf{R}_k$. Then

i) If $\mathcal{F}$ is invertible, then $\mathcal{F} \not\equiv f_k(0) \bmod k$.

ii) If k is prime and $\mathcal{F} \not\equiv f_k(0) \bmod k$, then $\mathcal{F}$ is invertible.

Proof: Let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. If $\mathcal{F}$ is invertible, then by R17.1.2 x_1 is invertible mod k so that $x_1 \neq k$. By R20.37 $\mathcal{F} \not\equiv f_k(0) \bmod k$. If $\mathcal{F} \not\equiv f_k(0) \bmod k$, by R20.37 $x_1 \neq k$. If k is prime, since $x_1 \in \{1, 2, \ldots, k\}$, x_1 is invertible mod k. By R17.1.2 $\mathcal{F}$ is invertible.

Corollary R20.41 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G}, \mathcal{H}, \mathcal{I} \in \mathbf{R}_k$ with $\mathcal{F} \equiv \mathcal{G} \bmod k^t$ and $\mathcal{H} \equiv \mathcal{I} \bmod k^t$. Then

i) $\mathcal{F} + \mathcal{H} \equiv \mathcal{G} + \mathcal{I} \bmod k^t$.

ii) $\mathcal{F} \cdot \mathcal{H} \equiv \mathcal{G} \cdot \mathcal{I} \bmod k^t$.

iii) $-\mathcal{F} \equiv -\mathcal{G} \bmod k^t$.

Proof: Let $\mathcal{F}, \mathcal{G}, \mathcal{H}, \mathcal{I}$ in $\mathbf{R}_k$ be associated with $\{w_n\}, \{x_n\}, \{y_n\}, \{z_n\}$ respectively. By hypothesis and R20.37, $w_t = x_t$ and $y_t = z_t$. Let $\mathcal{F} + \mathcal{H}$ and $\mathcal{G} + \mathcal{I}$ be associated with $\{u_n\}$ and $\{v_n\}$ respectively. By R12.4.4 $u_t \equiv w_t + y_t$ and $v_t \equiv x_t + z_t$, both mod k^t. Since $w_t = x_t$ and $y_t = z_t$, $u_t \equiv v_t \bmod k^t$. Since $u_t, v_t \in \{1, 2, \ldots, k^t\}$, $u_t = v_t$. Part i) now follows from R20.37. Part ii) follows similarly, as does part iii), with the use of R12.6.2.

Corollary R20.42 Let $k \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$. Assume $\mathcal{F} \equiv \mathcal{G} \bmod k^t$ for all $t \in \mathbb{N}$. Then $\mathcal{F} = \mathcal{G}$.

Proof: Let $\mathcal{F}, \mathcal{G}$ in $\mathbf{R}_k$ be associated with $\{x_n\}, \{y_n\}$ respectively. The hypothesis and R20.37 yield $x_t = y_t$ for all $t \in \mathbb{N}$. By R10.2.4 $\mathcal{F} = \mathcal{G}$.

In the rest of this section congruent elements mod k^t will be regarded as approximations of each other and congruent elements mod k^{t+1} as a better or improved approximations. (These ideas are intuitively appealing in the formal series representation of p-adic numbers.) Of particular interest are natural number approximations of elements in $\mathbf{R}_k$. The next two corollaries relate a frequently used tool to this point of view.

Corollary R20.43 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. Then $f_k(x_t) \equiv \mathcal{F} \bmod k^t$.

Proof: $f_k(x_t)$ is associated with $\{y_n\}$, where $y_n \equiv x_t \bmod k^n$ for all n. Since x_t and y_t are both in $\{1, 2, \ldots, k^t\}$, $y_t = x_t$ and so $f_k(x_t) \equiv \mathcal{F} \bmod k^t$ by R20.37.

Proposition R20.44 Let $k \in \mathbb{N}$ with $k \geq 2$, let $\mathcal{F} \in \mathbf{R}_k$, and let $\{\mathcal{F}_i\}$ be a sequence in $\mathbf{R}_k$. Then $\{\mathcal{F}_i\}$ converges to $\mathcal{F}$ in $\mathbf{R}_k$ if and only if for every $t \in \mathbb{N}$ $\mathcal{F}_i \equiv \mathcal{F} \bmod k^t$ eventually in i.

Proof: Let $\mathcal{F}_i$ be associated with $\{{}^i x_n\}$ and $\mathcal{F}$ with $\{y_n\}$. Assume for every $t \in \mathbb{N}$ $\mathcal{F}_i \equiv \mathcal{F} \bmod k^t$ eventually in i and let $m \in \mathbb{N}$. There exists j such that $i \geq j$ implies $\mathcal{F}_i \equiv \mathcal{F} \bmod k^m$. By R20.37 $i \geq j$ implies ${}^i x_m = y_m$. By R17.2.16 this shows $\{\mathcal{F}_i\}$ converges to $\mathcal{F}$ in $\mathbf{R}_k$. Now assume convergence and let $t \in \mathbb{N}$. By the other half of R17.2.16 there is j such that $i \geq j$ implies ${}^i x_t = y_t$, i.e., $\mathcal{F}_i \equiv \mathcal{F} \bmod k^t$ by R20.37.

Corollary R20.45 Let $k \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F} \in \mathbf{R}_k$ be associated with $\{x_n\}$. Then the sequence $\{f_k(x_i)\}$ converges to $\mathcal{F}$ in $\mathbf{R}_k$.

Proof: For each $t \in \mathbb{N}$ and $i \geq t$, $f_k(x_i) \equiv \mathcal{F} \bmod k^i$ by R20.43 and so $f_k(x_i) \equiv \mathcal{F} \bmod k^t$ by R20.35. By R20.44 $\{f_k(x_i)\}$ converges to $\mathcal{F}$ in $\mathbf{R}_k$.

Lemma R20.46 Let $k, t \in \mathbb{N}$ with $k \geq 2$. Let $\mathcal{F}, \mathcal{G} \in \mathbf{R}_k$ with $\mathcal{F} = f_k(k^t) \cdot \mathcal{G}$. Then $\mathcal{F} \equiv f_k(0) \bmod k^t$.

Proof: Let $\mathcal{F}, \mathcal{G}, f_k(t)$ be associated with $\{x_n\}, \{y_n\}, \{z_n\}$ respectively. Then $z_t = k^t$ and $x_t \equiv y_t k^t \bmod k^t$. Since $x_t \in \{1, 2, \ldots, k^t\}$, $x_t = k^t$. Since $f_k(0)$ is associated with $\{k^n\}$, by R20.37 $\mathcal{F} \equiv f_k(0) \bmod k^t$.

Robert [1 ; p. 46] describes the second principle of Hensel's Philosophy as a technique of finding roots of polynomials in the ring of p-adic integers. He illustrates this technique with a version of Newton's method. A reworking of his illustration for $\mathbf{R}_p$, with p prime, concludes this section. In brief it involves a two-step process: first, approximate a root in $\mathbf{R}_p \bmod p^t$ and secondly, take the limit to obtain a root in $\mathbf{R}_p$.

Let P be in $A[X]$, where A is a commutative ring with unity. The derivative of P will be denoted by the standard P', which can be defined algebraically in the expected way for a polynomial. The Taylor's formulas for P can be derived by straightforward algebra, e.g., the second-order formula

$$P(a + h) = P(a) + h \cdot P'(a) + h^2 \cdot Q(a, h),$$

where $Q \in A[X, Y]$, and the first-order formula

$$P(a + h) = P(a) + h \cdot Q_1(a, h),$$

where $Q_1 \in A[X, Y]$.

Lemma R20.47 Let p be a prime and let $\mathcal{F} \neq f_p(0)$ be in $\mathbf{R}_p$. Let $m = \text{rord}(\mathcal{F})$. Then there is an invertible $\mathcal{I} \in \mathbf{R}_p$ such that $\mathcal{F} = f_p(p^m) \cdot \mathcal{I}$.

Proof: This is a restatement of R17.1.10 using R20.8 and notation introduced in R20.7 and R16.6.

Lemma R20.48 Let p be a prime, $t \in \mathbb{N}$, and $\mathcal{F} \in \mathbf{R}_p$ with $\mathcal{F} \equiv f_p(0) \bmod p^t$. Then there is $\mathcal{F}_1 \in \mathbf{R}_p$ such that $\mathcal{F} = f_p(p^t) \cdot \mathcal{F}_1$.

Proof: If $\mathcal{F} = f_p(0)$, let $\mathcal{F}_1 = f_p(0)$. If $\mathcal{F} \neq f_p(0)$, let $\mathcal{F}$ be associated with $\{x_n\}$. By R20.37 $x_t = k^t$ so that $t \leq m$, where $m = \text{rord}(\mathcal{F})$. By R20.47 $\mathcal{F} = f_p(p^m) \cdot \mathcal{I}$ and so $\mathcal{F}_1 = f_p(p^{m-t}) \cdot \mathcal{I}$ has the desired property.

Lemma R20.49 Let p be a prime and $\mathcal{F}, \mathcal{I} \in \mathbf{R}_p$ with $\mathcal{I}$ invertible and $\mathcal{F}$ not invertible. Then $\mathcal{I} + \mathcal{F}$ is invertible.

Proof: If $\mathcal{F} = f_p(0)$, the conclusion clearly holds. Thus assume $\mathcal{F} \neq f_p(0)$ and $\mathcal{H} = \mathcal{I} + \mathcal{F}$ is not invertible. Since $\mathcal{I}$ is invertible, $\mathcal{H} \neq f_k(0)$. By R20.16ii $|\mathcal{F}|, |\mathcal{H}| < 1$ so that $\text{rord}(\mathcal{F})$, $\text{rord}(\mathcal{H}) \geq 1$. By R20.47 there are $s, t \in \mathbb{N}$ and $\mathcal{I}_1, \mathcal{I}_2 \in \mathbf{R}_p$ such that $\mathcal{F} = f_p(p^s) \cdot \mathcal{I}_1$ and $\mathcal{H} = f_p(p^t) \cdot \mathcal{I}_2$. Then $\mathcal{I} = \mathcal{H} - \mathcal{F} = f_p(p) \cdot \mathcal{H}_1$ where $\mathcal{H}_1 \in \mathbf{R}_p$. By R20.13iv $|\mathcal{I}| = |f_p(p)| \cdot |\mathcal{H}_1|$. Since $|f_p(p)| = 1/2$ and $|\mathcal{H}_1| \leq 1$, $|\mathcal{I}| \leq 1/2$. By R20.16ii $\mathcal{I}$ is not invertible, a contradiction.

A division operation sometimes makes sense within $\mathbf{R}_p$ even without constructing the qoutient field of the integral domain. One such case occurs in the following results. A

division notation will be used to maintain the form of Newton's method. As usual, p denotes a prime.

Notation: Let $P \in \mathbf{R}_p\,[X]$, $\mathcal{F} \in \mathbf{R}_p$, and $t \in \mathbb{N}$. Assume $P(\mathcal{F}) \equiv f_p(0) \bmod p^t$ and $P'(\mathcal{F}) \neq f_p(0)$. Let $m = \text{rord}(P'(\mathcal{F}))$. Let $P(\mathcal{F}) = f_p(p^t) \cdot \mathcal{F}_1$ as in R20.48 and $P'(\mathcal{F}) = f_p(p^m) \cdot \mathcal{I}$, where $\mathcal{I}$ is invertible, as in R20.47. If $m \leq t$, $P(\mathcal{F})/P'(\mathcal{F})$ will denote $f_p(p^{t-m}) \cdot \mathcal{F}_1 \cdot \mathcal{I}^{-1}$, which is in $\mathbf{R}_p$. Note that $|P(\mathcal{F})/P'(\mathcal{F})| \leq 1/p^{t-m}$ by R20.13iv and R20.16ii, since $|f_p(p^{t-m})| = 1/p^{t-m}$ and $|\mathcal{F}_1| \leq 1$.

Proposition R20.50 Let p be a prime, $P \in \mathbf{R}_p\,[X]$, $\mathcal{F} \in \mathbf{R}_p$, and $t \in \mathbb{N}$. Assume $P(\mathcal{F}) \equiv f_p(0) \bmod p^t$ and $P'(\mathcal{F}) \neq f_p(0)$. Let $m = \text{rord}(P'(\mathcal{F}))$ and assume $m < t/2$. Let $\mathcal{G} = \mathcal{F} - P(\mathcal{F})/P'(\mathcal{F})$. Then

i) $P(\mathcal{G}) \equiv f_p(0) \bmod p^{t+1}$.

ii) $\mathcal{G} \equiv \mathcal{F} \bmod p^{t-m}$.

iii) $P'(\mathcal{G}) \neq f_p(0)$ and $\text{rord}(P'(\mathcal{G})) = \text{rord}(P'(\mathcal{F}))$.

Proof: Using the notation just established and the second-order Taylor's formula, one has

$$P(\mathcal{G}) = P(\mathcal{F}) - P'(\mathcal{F}) \cdot f_p(p^{t-m}) \cdot \mathcal{I}^{-1} \cdot \mathcal{F}_1 + (f_p(p^{t-m}) \cdot \mathcal{I}^{-1} \cdot \mathcal{F}_1)^2 \cdot \mathcal{H},$$

where $\mathcal{H} \in \mathbf{R}_p$. Easy algebra yields $P(\mathcal{G}) = f_p(p^{2(t-m)}) \cdot \mathcal{H}_1$, where $\mathcal{H}_1 \in \mathbf{R}_p$. Since $m < t/2$, $2(t-m) \geq t+1$ and so $P(\mathcal{G}) \equiv f_p(0) \bmod p^{t+1}$ by R20.46. By R20.46 $P(\mathcal{F})/P'(\mathcal{F}) \equiv f_p(0) \bmod p^{t-m}$ and so by definition of $\mathcal{G}$, $\mathcal{G} \equiv \mathcal{F} \bmod p^{t-m}$. For the third part, apply the first-order Taylor formula to $P'(\mathcal{F} + (\mathcal{G} - \mathcal{F}))$ and obtain

$$P'(\mathcal{G}) = P'(\mathcal{F}) - (P(\mathcal{F})/P'(\mathcal{F})) \cdot \mathcal{H}_2,$$

where $\mathcal{H}_2 \in \mathbf{R}_p$. Using the underlying meaning just described in the paragraph on notation, we have $P'(\mathcal{G}) = f_p(p^m) \cdot \mathcal{I} - f_p(p^{t-m}) \cdot \mathcal{F}_1 \cdot \mathcal{I}^{-1} \cdot \mathcal{H}_2$. Since $m < t/2$, $m < t - m$ and so $P'(\mathcal{G}) = f_p(p^m)(\mathcal{I} - f_p(p^{t-2m}) \cdot \mathcal{F}_1 \cdot \mathcal{I}^{-1} \cdot \mathcal{H}_2)$. By R20.49 the second factor is invertible and so $P'(\mathcal{G}) \neq f_p(0)$. By R20.9 $\text{rord}(P'(\mathcal{G})) = m + \text{rord}(\mathcal{I} - f_p(p^{t-2m}) \cdot \mathcal{F}_1 \cdot \mathcal{I}^{-1} \cdot \mathcal{H}_2)$, since $\text{rord}(f_p(p^m)) = m$. By R20.16ii the second term is 0, which yields the desired equality.

R20.50 allows the iterative definition used in the next two results. Robert calls R20.52 Hensel's Lemma.

Lemma R20.51 Let p be a prime, $P \in \mathbf{R}_p\,[X]$, $\mathcal{F} \in \mathbf{R}_p$, and $t \in \mathbb{N}$. Assume $P(\mathcal{F}) \equiv f_p(0) \bmod p^t$ and $P'(\mathcal{F}) \neq f_p(0)$. Let $m = \text{rord}(P'(\mathcal{F}))$ and assume $m < t/2$. Let $\mathcal{G}_1 = \mathcal{F} - P(\mathcal{F})/P'(\mathcal{F})$ and, for all $j \in \mathbb{N}$, $\mathcal{G}_{j+1} = \mathcal{G}_j - P(\mathcal{G}_j)/P'(\mathcal{G}_j)$. Then the sequence $\{\mathcal{G}_j\}$ converges in $\mathbf{R}_p$.

Proof: By a routine induction, R20.50, and the obsevation at the end of the paragraph on notation, $P(\mathcal{G}_j) \equiv f_p(0) \bmod p^{t+j}$ and $|P(\mathcal{G}_j)/P'(\mathcal{G}_j)| \leq 1/p^{t+j-m}$. Thus $d_p(\mathcal{G}_{j+1}, \mathcal{G}_j) \leq 1/p^{t+j-m}$. By the triangle inequality, for all $l \in \mathbb{N}$

$$d_p(\mathcal{G}_{j+l}, \mathcal{G}_j) \leq \Sigma_{i=j}^{j+l-1} 1/p^{t+i-m} \leq 1/p^{t+j-m} \cdot p/(p-1).$$

It follows that $\{\mathcal{G}_j\}$ is Cauchy and so convergent in the compact $\mathbf{R}_p$.

Proposition R20.52 [Hensel's Lemma] Let p be a prime, $P \in \mathbf{R}_p\,[X]$, $\mathcal{F} \in \mathbf{R}_p$, and $t \in \mathbb{N}$. Assume $P(\mathcal{F}) \equiv f_p(0) \bmod p^t$ and $P'(\mathcal{F}) \neq f_p(0)$. Let $m = \text{rord}(P'(\mathcal{F}))$ and assume $m < t/2$. Let $\mathcal{G}_1 = \mathcal{F} - P(\mathcal{F})/P'(\mathcal{F})$ and, for all $j \in \mathbb{N}$, $\mathcal{G}_{j+1} = \mathcal{G}_j - P(\mathcal{G}_j)/P'(\mathcal{G}_j)$.

Let $\mathcal{H}$ be the limit of $\{\mathcal{G}_j\}$. Then $\mathcal{H}$ is the unique element of $\mathbf{R}_k$ such that $P(\mathcal{H}) = f_p(0)$ and $\mathcal{H} \equiv \mathcal{F} \bmod p^{t-m}$.

Proof: By a routine induction and R20.50, for all j $P(\mathcal{G}_j) \equiv f_p(0) \bmod p^{t+j}$ and $\mathcal{G}_j \equiv \mathcal{F} \bmod p^{t-m}$. The second condition combined with R17.2.16 and R20.37 shows that $\mathcal{H} \equiv \mathcal{F} \bmod p^{t-m}$. The first condition with R20.44 and R20.35 implies that $\{P(\mathcal{G}_j)\}$ converges to $f_p(0)$. Since P is continuous on $\mathbf{R}_p$, $\{P(\mathcal{G}_j)\}$ converges to $P(\mathcal{H})$. Thus $P(\mathcal{H}) = f_p(0)$. Now assume $\mathcal{H}_1 \in \mathbf{R}_p$ with $P(\mathcal{H}_1) = f_p(0)$ and $\mathcal{H}_1 \equiv \mathcal{F} \bmod p^{t-m}$. By R20.14 and R20.50iii $|P'(\mathcal{H})| = 1/p^m$. Apply the second-order Taylor formula:

$$P(\mathcal{H}_1) = P(\mathcal{H}) + P'(\mathcal{H})(\mathcal{H}_1 - \mathcal{H}) + (\mathcal{H}_1 - \mathcal{H})^2\mathcal{H}_2,$$

where $\mathcal{H}_2 \in \mathbf{R}_p$. Since $P(\mathcal{H}_1) = f_p(0) = P(\mathcal{H})$, $(\mathcal{H}_1 - \mathcal{H})(P'(\mathcal{H}) + (\mathcal{H}_1 - \mathcal{H})\mathcal{H}_2) = f_p(0)$. If $\mathcal{H}_1 \neq \mathcal{H}$, since $\mathbf{R}_p$ is an integral domain, by R20.13iii, $|(\mathcal{H}_1 - \mathcal{H})\mathcal{H}_2)| = |P'(\mathcal{H})| = 1/p^m$. Since $\mathcal{H} \equiv \mathcal{H}_1 \bmod p^{t-m}$ and $m < t/2$ so that $m + 1 \leq t - m$, by R20.35 $\mathcal{H} \equiv \mathcal{H}_1 \bmod p^{m+1}$. By R20.48 $\mathcal{H}_1 - \mathcal{H} = f_p(p^{m+1}) \cdot \mathcal{H}_3$ and so $|(\mathcal{H}_1 - \mathcal{H})| \leq 1/p^{m+1}$. Thus $|(\mathcal{H}_1 - \mathcal{H})\mathcal{H}_2)| \leq 1/p^{m+1}$, a contradiction.

Robert [1; pp. 49-54] describes several concrete applications of Hensel's Lemma: finding inverses and roots of unity in $\mathbf{R}_p$, as well as applications in the field of quotients.

Albert J. Klein 2010
http://www.susanjkleinart.com/compactification/

References

1. Robert, Alain M., A Course in p-adic Analysis, Springer Verlag, New York, 2000.
2. This Website, R10: Some Metric Compactifications of the Natural Numbers
3. This Website, R12: Extension of Arithmetic Operations
4. This Website, R16: The Remnant Rings as Compactifications
5. This Website, R17: Algebraic Structure of the Remnant Rings