Chapter X

Discrete valuation rings

[Reference: Matsumura, "Commutative ring Theory" Cambridge Univ. Press Ch. 4]

Goal: we will define and study a class of local rings which turn out to be essential tools in algebraic geometry and number theory, despite looking very special at first sight...

1 - Valuations

Definition - Let R be a ring. A (rank 1) valuation v on R is a map $v : R \longrightarrow \mathbb{R} \cup \{+\infty\}$ (ordered in the obvious way) such that:

(i) $v(x) = +\infty \iff x = 0$

(ii) $v(xy) = v(x) + v(y)$ for x, y in R (with the convention $x + \infty = +\infty$)

(iii) $v(x+y) \geq \min(v(x), v(y))$ for x, y in R (with the convention $\min(x, +\infty) = x$)

Example – Let R be a UFD and $p \in R$ an irreducible element. Define $v_p : R \longrightarrow \mathbb{Z} \cup \{+\infty\}$ by

$$v_p(b) = \max\{ k \geq 0 \mid p^k \mid b \}$$

$$= \text{"the power of } p \text{ in the factorization of } b\text{"}$$

Then v_p is a valuation on R, called the "p-adic valuation". In other words, $v_p(b) \geq k$ means that $b = p^k c$ for some $c \in R$, and $v_p(b) = k$ means in addition that $p \nmid c$. From this, it is easy to see that v_a is indeed a valuation. For instance, taking $R = \mathbb{Z}$, we get the p-adic valuations (e.g. $v_3(63) = 2$) for any prime number p. For a field K, we can take $R = K[x]$, $f \in R$ irreducible and get the f-adic valuation; if $f = x - t$ for $t \in K$, this is the order of vanishing of a polynomial at the point t.

Lemma. Let v be a valuation on R. Then R is an integral domain and v extends uniquely to a valuation on $\mathrm{Frac}(R)$ such that

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

for (a, b) in $K \times K^{\times}$.

Conversely, if v is a valuation on K, then its restriction to any subring $A \subset K$ is a valuation on A.

Proof. If x, y are non-zero then $v(xy) = v(x) + v(y)$ is in $\mathbb{R}$ so $xy \neq 0$ by condition (i). So R is an integral domain.

To check that v extends to $\mathrm{Frac}(R)$, we first check that defining $v\left(\frac{a}{b}\right) = v(a) - v(b)$ is well-defined: if $\frac{a}{b} = \frac{c}{d}$, then $ad = bc$ so $v(a) + v(d) = v(b) + v(c)$, which gives the result. Then we have $v\left(\frac{a}{b}\right) = +\infty \iff v(a) = +\infty$

$\Leftrightarrow \quad a = 0 \quad \Leftrightarrow \quad \frac{a}{b} = 0$, and moreover

$$v\left(\frac{a}{b} \cdot \frac{c}{d}\right) = v(a) + v(c) - v(b) - v(d)$$

$$= v\left(\frac{a}{b}\right) + v\left(\frac{c}{d}\right)$$

$$v\left(\frac{a}{b} + \frac{c}{d}\right) = v(ad + bc) - v(b) - v(d)$$

$$\geq \min\left(v(ad), v(bc)\right) - v(b) - v(d)$$

$$= \min\left(v(a) + v(d), v(b) + v(c)\right) - v(b) - v(d)$$

$$= \min\left(v(a) - v(b), v(c) - v(d)\right).$$

The final property is clear.

□

Definition - R ring, v valuation on R.

The **value group** of v is the subgroup

$$\Gamma_v = v\left(\mathrm{Frac}(R)^\times\right) \subset \mathbb{R}$$

(v: the extension of v to $\mathrm{Frac}(R)$)

The valuation v is called a **discrete** valuation if $\Gamma_v \subset \mathbb{R}$ is discrete, or equivalently if there exists $\alpha \in \mathbb{R}$ s.t. $\Gamma_v = \alpha\mathbb{Z}$. It is

normalized if one can choose $\alpha = 1$, i.e. $\Gamma_v = \mathbb{Z}$.

Note. We used the following fact: a subgroup $\Gamma \subset \mathbb{R}$ is discrete if and only if there exists $\alpha \in \mathbb{R}$ such that $\Gamma = \alpha\mathbb{Z}$. (Indeed, if Γ is not just $\{0\}$, there is a smallest $\alpha > 0$ in Γ, and using an argument similar to euclidean division, one checks that $\Gamma = \alpha\mathbb{Z}$.)

Example. The p-adic valuations of the previous example are normalized discrete valuations (with $v_p(p) = 1$). We will concentrate on these, but here is a simple example of a valuation which is not discrete: let $R = \mathbb{C}[x, y]$ and

$$v\left(\sum a_{m,n} x^m y^n\right) = \min\{m + \sqrt{2}n \mid a_{m,n} \neq 0\}$$

Then one sees that $\Gamma_v = \mathbb{Z} + \sqrt{2}\mathbb{Z} \subset \mathbb{R}$, which is not discrete (because $\sqrt{2} \notin \mathbb{Q}$).

2 - Valuation rings

Lemma - Let v be a valuation on a ring R, and $K = \mathrm{Frac}(R)$. Denote by v the extension of v to K. Then the set

$$R_v = \{ x \in K \mid v(x) \geq 0 \}$$

is a subring of K, called the valuation ring of v. It is a local ring with maximal ideal

$$m_v = \{ x \in K \mid v(x) > 0 \}$$ and fraction field K.

If $\Gamma_v \neq \{0\}$ then $m_v \neq \{0\}$, $R_v \neq K$.

Proof - If x, y are in R_v then

$$v(xy) = v(x) + v(y) \geq 0 \quad \text{so} \quad xy \in R_v$$

$$v(x+y) \geq \min(v(x), v(y)) \geq 0 \quad \text{so} \quad x+y \in R_v$$

which proves that $R_v \subset K$ is a subring.

If $x \in R_v$ and $y \in m_v$, then $v(xy) \geq v(y) > 0$ so $xy \in m_v$; if $x \in m_v$ also then

$$v(x+y) \geq \min(v(x), v(y)) > 0$$

so $x+y \in m_v$; this means that $m_v \subset R_v$ is an ideal. We have $m_v \neq R_v$ when $\Gamma_v \neq \{0\}$.

Moreover, if $x \in R_v - \{0\}$, then

$$v(x^{-1}) = -v(x)$$

so $x^{-1} \in R_v$ if and only if $v(x) = 0$. This implies that $R_v^\times = R_v - m_v$, which we saw in Chapter 3 is a characterization of a local ring with maximal ideal m_v (indeed, if $I \subset R_v$ is an ideal not contained in m_v, then it contains x with $v(x) = 0$, so $x \in R_v^\times$, so $I = R_v$).

Let $x \in K$. Then either $x \in R_v$ or $v(x) < 0$, in which case $\frac{1}{x} \in R_v$ and $x = \frac{1}{1/x} \in \mathrm{Frac}(R_v)$.

Finally, $\Gamma_v \neq \{0\}$ implies $R_v \neq K$. □

Definition - A (rank 1) valuation ring is a pair (R, v) of a ring with a valuation such that R is the valuation ring R_v. A discrete valuation

ring (or DVR) is a valuation ring (R, v) with v discrete and $\Gamma_v \neq \{0\}$; it is normalized if $\Gamma_v = \mathbb{Z}$.

Examples - For a UFD R and $p \in R$ irreducible, the valuation ring of the p-adic valuation v_p is the localization R_{pR} of R with respect to the prime ideal pR.

Indeed, for $x = \frac{a}{b} \in \mathrm{Frac}(R)$, we have $x \in R_{v_p} \iff v_p(a) \geq v_p(b)$. But if we factor $a = p^{v_p(a)} a'$, $b = p^{v_p(b)} b'$ with $p \nmid a'$ and $p \nmid b'$, we get

$$x = \frac{p^{v_p(a) - v_p(b)} a'}{b'} \in R_{pR}$$

since $b' \notin pR$. Conversely, if $x = \frac{a}{b}$ with $b \notin pR$, $a \in R$, then $v_p(x) = v_p(a) - v_p(b)$

$$= v_p(a) \geq 0.$$

Definition - If (R, v) is a discrete valuation ring, then any element $\pi \in R$ such that $v(\pi)$

generates Γ_v (which is $\simeq \mathbb{Z}$) is called a uniformizer of R. If v is normalized, this means that

$$v(\pi) = 1.$$

Example - (1) For the valuation ring associated to an irreducible element p of a UFD, p itself is a uniformizer.

(2) For an arbitrary DVR R, given a uniformizer π, all other uniformizers are of the form $u\pi$, where $u \in R_v^\times$, i.e., $v(u) = 0$.

The following lemma is very useful:

Lemma - Let v be a valuation on a ring R.

For x, y in R such that $v(x) \neq v(y)$, we have $v(x+y) = \min(v(x), v(y))$.

Proof - We may assume that $v(x) < v(y)$ and we need to check that $v(x+y) = v(x)$. We have then $x \neq 0$ and we write $x + y = x\left(1 + \frac{y}{x}\right)$

in $K = \mathrm{Frac}(R)$. In fact, $\frac{y}{x} \in m_v$ because of the assumption, so $1 + \frac{y}{x} \in R_v$. But it cannot be in m_v (otherwise $1 \in m_v$) so $1 + y/x \in R_v - m_v$ has valuation 0. Hence

$$v(x+y) = v(x) + v\left(1 + \frac{y}{x}\right) = v(x).$$

□

Proposition. Let (R, v) be a valuation ring. Then R is integrally closed.

Proof. Let x be an element of $\mathrm{Frac}(R)^\times$ integral over R and

$$x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

an equation satisfied by x, with $a_i \in R$.

If $x \notin R$, then $x^{-1} \in m_v$ since $v(x^{-1}) = -v(x) > 0$.

Multiplying the equation by x^{-n}, we get

$$1 + \underbrace{\frac{a_{n-1}}{x} + \dots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n}}_{\in m_v} = 0,$$

which is impossible since $1 \notin m_v$.

□

3- Characterizations of DVRs among valuation rings

We will explain in this section how to characterize DVRs among all valuation rings. In the next section, we will extend this to characterize them among all rings.

First a general fact:

Prop. Let (R, v) be a valuation ring.

(1) The set of ideals in R is totally ordered for inclusion (if I, J are ideals, then $I \subset J$ or $J \subset I$).

(2) $\dim(R) = 1$ if $\Gamma_v \neq \{0\}$.

Proof. (1) Let I and J be ideals in R and $y \in J$. If there exists $x \in I$ such that $v(x) \leq v(y)$ then $y = x \cdot \left(\frac{y}{x}\right) \in I$. ($\frac{y}{x} \in R_v$) So if J is not contained in I, there exists $y_0 \in J$ such that $v(x) > v(y_0)$ for all $x \in I$. But then for any $x \in I$, we have $x = y_0 \left(\frac{x}{y_0}\right) \in J$, i.e. $I \subset J$. ($\frac{x}{y_0} \in m_v$)

(2) Since R is a local ring and an integral domain which is not a field if $\Gamma_v \neq \{0\}$, we get a chain $\{0\} \subsetneq m_v$ of prime ideals in R, so $\dim(R) \geq 1$.

Let $p \neq \{0\}$ be a prime ideal. Let $x \in p - \{0\}$ and $\alpha = v(x) > 0$. Let $y \in m_v$; then $v(y) > 0$ so there exists an integer $n \geq 1$ such that

$$v\left(\frac{y^n}{x}\right) = n\,v(y) - \alpha \geq 0$$

hence $y^n = x \cdot \frac{y^n}{x} \in p$ ($\frac{y^n}{x} \in R_v$); since p is prime, this implies $y \in p$, hence $m_v \subset p$. This means that there are no other prime ideals than $\{0\}$ or m_v, and so $\dim(R) = 1$.

□

Note. In particular, a non-noetherian valuation ring will give an example of non-noetherian local ring with finite dimension.

[Matsumura 11.1]

Theorem - Let (R, v) be a valuation ring with $\Gamma_v \neq \{0\}$. The following conditions are equivalent:

(1) R is a DVR,

(2) R is a PID,

(3) R is noetherian.

(In particular, a valuation ring not DVR is not noetherian!)

Proof - (1) $\Rightarrow$ (2): suppose v is a discrete valuation with $\Gamma_v = \alpha\mathbb{Z}$, $\alpha > 0$; let π be a uniformizer in R. Let $I \subset R$ be an ideal, with $I \neq \{0\}$. Then $\{v(x) \mid x \in I - \{0\}\} \subset \alpha\mathbb{N}$ is not empty, hence has a smallest element $m\alpha$ with $m \geq 0$. We claim that $I = \pi^m R$. Indeed, if $x \in I$ then $v(x) = n\alpha$ with $n \geq m$, so $x = \pi^m \frac{x}{\pi^m}$ with $v\left(\frac{x}{\pi^m}\right) = (n-m)\alpha \geq 0$, hence $x \in \pi^m I$. Conversely, there exists $x_0 \in I$ with $v(x_0) = m\alpha$; then $\pi^m = x \frac{\pi^m}{x}$ with $v\left(\frac{\pi^m}{x}\right) = 0$, so $\pi^m \in I$.

(2) $\Rightarrow$ (3): any PID is noetherian.

(3) $\Rightarrow$ (1): if R is not a DVR, there is a sequence (α_n) in Γ_v such that

$$0 < \alpha_{n+1} < \alpha_n$$

for all n. Let $x_n \in R$ be such that $v(x_n) = \alpha_n$; then $x_n R \subset x_{n+1} R$ (since $x_n = x_{n+1} \frac{x_n}{x_{n+1}}$ and $\frac{x_n}{x_{n+1}} \in R$), and the inclusion is strict ($x_{n+1} \notin x_n R$, since otherwise $x_{n+1} = x_n y \Rightarrow \alpha_{n+1} \geq \alpha_n$) and hence the ring R is not noetherian.

□

4. Characterizing DVRs among rings

[Matsumura 11.2]

Theorem. Let R be a noetherian local ring with maximal ideal m, residue field $k = R/m$. The following are equivalent:

(1) for some v, (R, v) is a (normalized) DVR.

(2) R is integrally closed of dimension 1.

(3) $\dim(R) \geq 1$ and $\dim_k(m/m^2) = 1$.

(4) $\dim(R) \geq 1$ and m is principal.

(5) R is a PID and not a field.

Note that (1) $\Rightarrow$ (2), (4), (5) have already been shown. Further, (5) $\Rightarrow$ (4) since a PID which is not a field has dimension 1.

For the other implications, we will need an extra useful tool.

[Matsumura, 8.9 ; 8.10]

Theorem (Krull's Intersection Theorem)

Let R be a noetherian local ring with maximal ideal m. Then

$$\bigcap_{n \geq 0} m^n = \{0\}.$$

We will prove this later.

Proof that (4) $\Rightarrow$ (1): we need to construct the valuation, and the fact that $m = \pi R$ for some π gives us a clue. (Indeed, if R is a normalized DVR, one can check that $v(x)$ is the largest $k \geq 0$

such that $x \in \pi^k R$ but $x \notin \pi^{k+1} R$ ...) By Krull's Intersection Theorem, we have $\bigcap_{k \geq 0} m^k = \{0\}$ so for any $x \neq 0$ in R there is a unique integer $v(x) \geq 0$ such that $x \in m^k$ but $x \notin m^{k+1}$.

We define $v(0) = +\infty$. We then claim that v is a valuation on R:

(i) $v(x) = +\infty \iff x = 0$

(ii) $v(x+y) \geq \min(v(x), v(y))$ because

$x \in m^{v(x)}$, $y \in m^{v(y)} \Rightarrow x+y \in m^{\min(v(x),v(y))}$

(iii) if $x \neq 0$, $y \neq 0$ then $x \in m^{v(x)}$, $y \in m^{v(y)}$ implies $xy \in m^{v(x)+v(y)}$, so $v(xy) \geq v(x) + v(y)$.

If $xy \in m^{v(x)+v(y)+1} = \pi^{v(x)+v(y)+1} R$ then

$$\frac{x}{\pi^{v(x)}} \frac{y}{\pi^{v(y)}} \in \pi R = m$$

and since the factors are in R, and m is prime, either $\frac{x}{\pi^{v(x)}} \in \pi R$ or $\frac{y}{\pi^{v(y)}} \in \pi R$, neither of which is possible.

So v is a valuation; clearly $\Gamma_v \subset \mathbb{Z}$ and since $v(\pi) = 1$ (otherwise $\pi \in m^2$ so $m = m^2 = \dots$, contradicting the intersection theorem), we have $\Gamma_v = \mathbb{Z}$, so v is a normalized discrete valuation. To conclude, we need to check that $R = R_v$, when v is extended to $K = \mathrm{Frac}(R)$. But clearly $R \subset R_v$, and if $x = \frac{a}{b} \in R_v$, then $v(a) - v(b) \geq 0$, so there are a', b' in R such that $x = \frac{\pi^{v(a)} a'}{\pi^{v(b)} b'} = \pi^{v(a)-v(b)} \frac{a'}{b'}$; and since $b' \notin \pi R = m$, b' is a unit in R, so we get $x \in R$.

Proof that (2) $\Rightarrow$ (4): this is the trickiest part of the proof: we assume $\dim(R) = 1$ and R integrally closed, and we need to prove that m is principal. There is again a clear starting point: if the result is true, a generator is a uniformizer,

and any $\pi \in m - m^2$ should do. So we pick such a π (which exists since otherwise $m = m^2 = \dots$ again contradicts Krull's Intersection Theorem), and we will prove that $m = \pi R$ indeed.

Claim. There exists an injective R-linear morphism $R/m \xrightarrow{f} R/\pi R$.

This will be proved later. We assume this, and note then that there exists $x \in R$ such that $f(y) = xy + \pi R$ for $y \in R/m$, and the injectivity means that

$$m = \{ y \in R \mid xy \in \pi R \}. \qquad (*)$$

Let $a = \frac{x}{\pi}$; then for $y \in m$, we have

$$ay = \frac{xy}{\pi} \in R, \quad \text{so} \quad am \subset R.$$

We cannot have $am \subset m$, since otherwise the element a would be integral over R, so $a \in R$ since R is integrally closed, in which case

$x = a\pi \in \pi R$ would mean that $1 \in m$. Hence we have $am = R$ i.e. $xm = \pi R$. But then $x \in m$ is impossible (it would give $\pi \in m^2$), so $x \in R - m = R^\times$, and hence $m = \pi R$.

We now prove the Claim above. In fact, we will find $x \in R$ such that (*) above holds.

Consider the set of ideals of the form

$$I_x = \{ y \in R \mid xy \in \pi R \}$$

as x varies in $R - \pi R$. This is a non-empty set of ideals and $I_x \neq R$ for all $x \notin \pi R$. So there is a maximal element I_x, and $I_x \subset m$.

We claim that I_x is prime: indeed if $\alpha\beta \in I_x$ then $\alpha\beta x \in \pi R$; if $\beta \notin I_x$ then $\beta x \notin \pi R$, so $\alpha \in I_{\beta x}$, but $I_x \subset I_{\beta x}$ so that by maximality, we have $\alpha \in I_x$.

Since I_x is prime, either $I_x = \{0\}$ or $I_x = \{m\}$

(because $\dim R = 1$ so $\{0\} \subset m$ is a maximal chain of prime ideals); but $\pi \in I_x$ obviously, so $I_x \neq \{0\}$.

The proof of the theorem now only requires showing that (3) is equivalent to the other conditions. But Nakayama's Lemma shows that if $\pi + m^2$ generates m/m^2 as k-vector space, then π generates m, and the converse is clear.

□

Note - The construction in the proof of (2)⇒(4) is related to the theory of associated primes.

More generally, it is not difficult to adapt this proof to show that if M is a finitely-generated module over a noetherian ring R, then there is a sequence $\{0\} \subsetneq M_1 \subsetneq \cdots \subsetneq M_k = M$ such that $M_{i+1}/M_i \simeq R/p_i$ for some prime ideals p_i.

Example - Let $R = \mathbb{Z} \subset K = \mathbb{Q}$. What are the valuation rings in K (containing R necessarily)?

Let $v : \mathbb{Q} \longrightarrow \mathbb{R} \cup \{+\infty\}$ be a valuation with $\Gamma_v \neq \{0\}$. Note $v(n) \geq 0$ if $n \in \mathbb{Z}$.

Claim: there is a **unique** prime number p s.t.

$$v(x) = v_p(x)\, v(p)$$

for all $x \in \mathbb{Q}$, and $v(p) > 0$.

Indeed, consider $X = \{ p \mid v(p) > 0 \}$. We have $X \neq \emptyset$ (because otherwise $v(n) = 0$ for all $n \in \mathbb{Z} - \{0\}$, so $\Gamma_v = \{0\}$); and if we had **two** primes $p \neq q$ in X, then picking a and b in $\mathbb{Z}$ such that $ap + bq = 1$ we get

$$0 = v(1) \geq \min\left(v(p), v(q)\right) > 0$$

which is a contradiction. So $X = \{p\}$ for some prime.

Now for $n = p^{v_p(n)} q$ with q coprime to p, we get $v(n) = v_p(n)\, v(p)$.

5 - Krull's Intersection Theorem

The proof involves another technical but important tool.

[Matsumura 8.5]

Lemma. (Artin-Rees Lemma)

Let R be a noetherian ring, M a finitely-generated R-module, $N \subset M$ and let $I \subset R$ be an ideal. There exists $q \geq 0$ such that for all $n \geq q+1$,

$$I^n M \cap N = I^{n-q}(I^q M \cap N).$$

Proof. The inclusion $\supset$ is clear, so it is the converse which is interesting. We use a trick for this: let A be the R-module

$$A = \bigoplus_{n \geq 0} I^n \qquad [\text{with } I^0 = R]$$

and note that one can define a ring structure on A by the obvious multiplication $I^n \times I^m \to I^{n+m}$. This ring is an R-algebra, and it is noetherian: indeed, let $(x_1, \dots, x_k)$ be a generating set of

the ideal I. Then the elements $f(x_1, \dots, x_k)$ where f is a monomial of degree n generate I^n, hence there is a morphism

$$\begin{cases} R[X_1, \dots, X_k] \longrightarrow A \\ X_i \longmapsto x_i \end{cases}$$

which is a surjective morphism of R-algebras. So A is a finitely-generated K-algebra, and therefore noetherian.

Next let $\tilde{M} = \bigoplus_{n \geq 0} I^n M$; this is naturally an A-module via $I^{n_1} \times I^{n_2} M \longrightarrow I^{n_1+n_2} M$.

It is finitely-generated, hence noetherian: indeed, if $(m_1, \dots, m_\ell)$ generate M as R-module, then they generate $\tilde{M}$ as A-module (viewing M as $I^0 M \subset \tilde{M}$): if $a \in I^n$, $m \in M$, then am in $I^n M \subset \tilde{M}$ is of the form $\sum_{i=1}^{\ell} \underbrace{(a_i a)}_{\in I^n} m_i$.

Now let

$$\tilde{N} = \bigoplus_{n \geq 0} (I^n M \cap N) \subset \tilde{M}$$

which is an A-submodule of $\tilde{M}$. As such, it is finitely-generated, and by taking the components of a generating set in the subspaces $I^n M$, we can find a generating set $\{y_1, \dots, y_s\}$ with $y_i \in I^{q_i} M \cap N$ for some $q_i \geq 0$.

Let $q = \max(q_i)$.

For $n \geq q$ and $y \in I^n M \cap N$, we can write

$$y = \sum_{i=1}^{s} a_i y_i \in I^n M \cap N$$

with $a_i \in A$; looking at the way multiplication works on $A \times \tilde{M}$, this in fact implies that $a_i \in I^{n-q_i}$. Using $I^{n-q_i}(I^{q_i} M \cap N) \subset I^{n-q}(I^q M \cap N)$, we conclude $y \in I^{n-q}(I^q M \cap N)$. □

Proof of the intersection theorem. More generally, let M be a finitely-generated R-module (instead of just $M = m \subset R$ the maximal ideal).

Let $N = \bigcap_{n \geq 0} m^n M \subset M$. We apply the Artin-Rees lemma to $N \subset M$: there exists $q \geq 0$ such that

$$m^n M \cap N = m^{n-q}(m^q M \cap N)$$

for all $n \geq q$. But $m^n M \cap N = N$ for all n, so this means $N = m^{n-q} N$ for $n \geq q$. Taking $n = q+1$ and applying Nakayama's lemma, we get $N = 0$.

□

6 - Completion

We are now going to do something quite surprising in appearance: we will do analysis with algebra. More precisely, a valuation gives rise to a topology, and by looking at the corresponding completion, we will get some very new and remarkable rings. We will then present some of their applications.

Proposition - Let v be a valuation on R. Define

$$\begin{cases} \|x\|_v = 2^{-v(x)} & \text{if } x \neq 0 \\ \|0\|_v = 0 \end{cases}$$

and define $d_v(x,y) = \|x-y\|_v$. Then

(1) $\|xy\|_v = \|x\|_v \|y\|_v$

(2) $\|x+y\|_v \leq \max(\|x\|_v, \|y\|_v) \leq \|x\|_v + \|y\|_v$

(3) d_v is a metric on R, and addition and multiplication are continuous (with $R \times R$ given the product topology).

Proof - (1) and (2) follow immediately from $v(xy) = v(x) + v(y)$ and $v(x+y) \geq \min(v(x), v(y))$.

Then it is straightforward that d_v is a metric:

for instance $d_v(x,y) = \|x-y\|_v$

$$= \|(x-z)+(z-y)\|_v$$

$$\leq \|x-z\|_v + \|z-y\|_v$$

$$= d_v(x,z) + d_v(z,y)$$

proves the triangle inequality.

Then $d_v(x+y, x_0+y_0) = \|(x-x_0)+(y-y_0)\|_v$

$$\leq \|x-x_0\|_v + \|y-y_0\|_v$$

shows that $+$ is continuous and

$$d_v(xy, x_0y_0) = \|xy - x_0y_0\|_v$$

$$= \|x(y-y_0) + (x-x_0)y_0\|_v$$

$$\leq \|x\|_v \|y-y_0\|_v + \|x-x_0\|_v \|y_0\|_v$$

implies that multiplication is continuous.

□

Example. Let p be a prime number. Then for $\mathbb{Z}$ with the p-adic valuation v_p, a sequence $(n_k)_{k\geq 0}$ of integers converges to 0 if and only if $\|n_k\|_{v_p} \to 0$, if and only if $v_p(n_k) \to +\infty$, which means that the exponent of p in n_k goes to infinity. For instance:

$p^k \xrightarrow[k\to\infty]{} 0$; $k! \xrightarrow[k\to]{} 0$; $\frac{1}{k}$ diverges.

Remark. Geometrically, the metric defined by a valuation v has very striking and seemingly counterintuitive properties when one is used only to classical euclidean geometry.

Here are two key differences, both related to the version of the triangle inequality in $\mathbb{R}$, namely

$$d_v(x,z) \leq \max\left(d_v(x,y), d_v(y,z)\right)$$

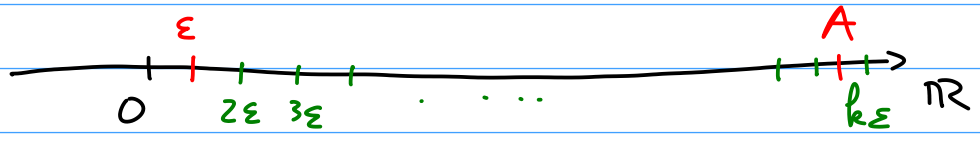
[which is called non-archimedean]

(1) Suppose $\|x\|_v = d_v(0,x) \leq 1$; then for any integer $k \geq 1$, we get

$$\|kx\|_v = \|\underbrace{x + \dots + x}_{k \text{ times}}\|_v \leq \|x\|_v \leq 1$$

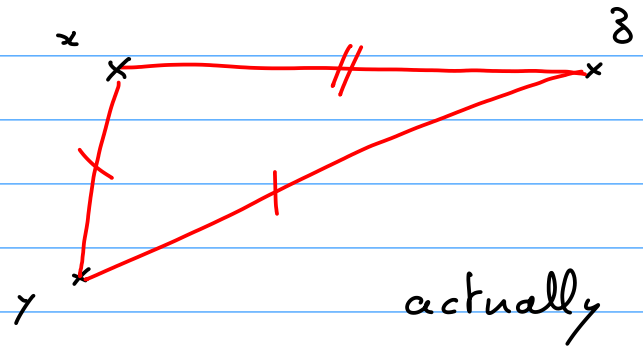
so no multiple of x "escapes" from the ball with radius 1, even if $x \neq 0$ [this explains the terminology "non-archimedean", since the so-called "archimedean principle" is the fact that for real numbers $\varepsilon > 0$ and $A > 0$, we can always

find an integer $k \geq 1$ such that $k\varepsilon > A$, however small ε is or large A is:



(2) Consider a "triangle" in R, in other words three different points x, y, z in R.

Then there are at least <u>two sides</u> of this triangle of the same length: if $d_v(x,z) \neq d_v(y,z)$, then the triangle inequality actually becomes



$$d_v(x,y) = \max\left(d_v(x,z), d_v(y,z)\right)$$

[because $v(x-y) = \max\left(v(x-z), v(z-y)\right)$ in that case], so $d_v(x,y)$ is either equal to $d_v(x,z)$ or to $d_v(y,z)$!

Such facts show that one needs to form brand new intuition for such geometry!

In general, the metric defined on R by a valuation is not <u>complete</u>: there are Cauchy sequences which do not converge. However, one can complete R in the same way that $\mathbb{R}$ is defined by completing $\mathbb{Q}$, using equivalence classes of Cauchy sequences. There is however a more concrete presentation/interpretation.

<u>Theorem.</u> Let (R, v) be a <u>discrete</u> valuation ring with maximal ideal m, uniformizer $\pi \in R$, residue field $R/\pi R$. Let

$$\hat{R} = \left\{ (x_k)_{k\geq 1} \;\middle|\; x_k \in R/\pi^k R \text{ for } k \geq 1,\ x_{k+1} \equiv x_k \bmod \pi^k R,\ k \geq 1 \right\}$$

with coordinate-wise addition and multiplication.

Further, for $x = (x_k) \in \hat{R}$, define

$$\hat{v}(x) = \begin{cases} +\infty, & x = 0 \\ \min\{ k \geq 1 \mid x_k \neq 0 \} - 1, & x \neq 0 \end{cases}$$

(so $\hat{v}(x) = k \geq 0$ if $x_1 = \dots = x_k = 0$, $x_{k+1} \neq 0$)

Then :

(1) $\hat{R}$ is a local ring with maximal ideal $\hat{m} = \{ (x_k) \mid x_1 = 0 \}$ and with $\begin{cases} \hat{R}/\hat{m} \xrightarrow{\sim} R/\pi R \\ (x_k) \longmapsto x_1 \end{cases}$.

(2) $(\hat{R}, \hat{v})$ is a normalized DVR with uniformizer $\hat{\pi} = (x_k)$ defined by $x_k = \pi + \pi^k R$ for all $k \geq 1$.

(2) The map $R \xrightarrow{i} \hat{R}$ such that $i(x) = (x + \pi^k R)_{k \geq 1}$ is an injective isometric morphism $(\| i(x) \|_{\hat{v}} = \| x \|_v)$ with dense image.

(3) The metric $d_{\hat{v}}$ on $\hat{R}$ is complete.

(4) The fraction field of $\hat{R}$ is $\hat{R}\left[\frac{1}{\hat{\pi}}\right]$ and is the completion of $\mathrm{Frac}(R) = R\left[\frac{1}{\pi}\right]$.

Proof — (1) It is elementary that $\hat{R}$ is a ring, and that $\hat{v}(x) = +\infty$ if and only if $x = 0$. Also if $\hat{v}(x) = v$ $\hat{v}(y) = w$, then $x_k + y_k = 0$ for $k \leq \min(v, w)$ so $\hat{v}(x+y) \geq \min(v, w)$.

For the product, consider k, $1 \leq k \leq v+w$. We can write $k = a + b$ with $0 \leq a \leq v$, $0 \leq b \leq w$. Then

$$\begin{cases} x_k \equiv x_a \bmod \pi^a = 0 \bmod \pi^a \\ y_k \equiv y_b \bmod \pi^b = 0 \bmod \pi^b \end{cases}$$

by the definition of the elements in $\hat{R}$. So

$$\begin{aligned} x_k \, y_k &\equiv 0 \bmod \pi^{a+b} \\ &= 0 \bmod \pi^k \end{aligned}$$

which shows that $\hat{v}(xy) \geq v + w$. And for $k = v + w + 1$, note that

$$\begin{cases} x_{v+w+1} \equiv 0 \bmod \pi^v \\ \quad\quad \not\equiv 0 \bmod \pi^{v+1} \\ y_{v+w+1} \equiv 0 \bmod \pi^w \\ \quad\quad \not\equiv 0 \bmod \pi^{w+1} \end{cases}$$

so that one can write

$$\begin{cases} x_{v+w+1} \equiv a\,\pi^v + b\,\pi^{v+1}, & \pi \nmid a \\ y_{v+w+1} \equiv c\,\pi^w + d\,\pi^{w+1}, & \pi \nmid c \end{cases}$$

where a, b, c, d are in R. Then

$$x_{v+w+1}\, y_{v+w+1} \equiv ac\,\pi^{v+w} + \alpha\,\pi^{v+w+1}$$

for some $\alpha \in R$. Since $\pi \nmid ac$, this is non-zero

modulo π^{v+w+1}, which shows that $\hat{v}(xy) = v+w$.

Thus we have shown that $\hat{v}$ is a valuation on $\hat{R}$, and it is straightforward then that $\hat{v}$ is a normalized discrete valuation.

Let $\hat{m} = \{ x \in \hat{R} \mid \hat{v}(x) \geq 1 \} = \{ x \in \hat{R} \mid x_1 = 0 \}$.

Then the properties of valuations show that $\hat{m}$ is an ideal in $\hat{R}$, and since $\begin{array}{ccc} \hat{R} & \longrightarrow & R/\pi R \\ x & \longmapsto & x_1 \end{array}$ is surjective (because $(x + \pi^k R)_{k \geq 1} \longmapsto x + \pi R$) with kernel $\hat{m}$, it is a maximal ideal with $\hat{R}/\hat{m} \simeq R/\pi R$.

Furthermore we have $\hat{R}^\times = \hat{R} - \hat{m}$. Indeed, the inclusion $\hat{R}^\times \subset \hat{R} - \hat{m}$ is always true.

Conversely, given $x = (x_k)$ with $\hat{v}(x) = 0$, we have $x_1 \in (R/\pi R)^\times$, and we then use

Lemma - For $k \geq 2$, $(R/\pi^k R)^\times$ is the set of all $x \bmod \pi^k R$ such that $x \bmod \pi R \neq 0$.

(i.e. $x \bmod \pi R$ is invertible)

It follows that x_k is invertible in $R/\pi^k R$, and we can define $y = (x_k^{-1})_{k\geq 1} \in \hat{R}$ with clearly $xy = 1$, so x is invertible.

[Proof of the lemma: the ring $R/\pi^k R$ is a local ring, with maximal ideal $\pi R/\pi^k R$, since maximal ideals in $R/\pi^k R$ correspond to max. ideals in R containing $\pi^k R$, and πR is the only one...)

(2) The fact that $\hat{R}$ is the valuation ring associated to $\hat{v}$ (i.e. $\hat{R} = \{x \in \mathrm{Frac}(\hat{R}) \mid \hat{v}(x) \geq 0\}$) follows from the properties in (1) and the following fact: if $x \in \hat{R} - \{0\}$, then $x = \hat{\pi}^{\hat{v}(x)} u$ where $u \in \hat{R}^\times$. Indeed, it follows that if $x = \frac{a}{b} \in \mathrm{Frac}(\hat{R})$ satisfies $\hat{v}(x) \geq 0$ then $x = \hat{\pi}^{\hat{v}(x)} u v^{-1} \in \hat{R}$.

To check the claim, it suffices to prove that $\hat{m} = \hat{\pi}\hat{R}$, since then we can use induction on

$\hat{v}(x)$ (if $\hat{v}(x) = 0$, then $x \in \hat{R}^\times$; if $\hat{v}(x) \geq 1$,

then $x \in \hat{m}$ so $x = \hat{\pi} y$ with

$\hat{v}(y) = \hat{v}(x) - 1$, so we can apply induction)

Since $\hat{\pi}\hat{R} \subset \hat{m}$, we need to prove the converse.

Let $x = (x_k) \in \hat{m}$, so $x_1 = 0 \in R/_\pi$, and

$x_k \equiv 0 \mod \pi R$ for $k \geq 2$. So we can write

$$x_k = \pi y_k + \pi^k R \quad , \quad y_k \in R, \ k \geq 2.$$

The elements y_k is well-defined modulo $\pi^{k-1}R$

and $y_{k+1} \equiv y_k \mod \pi^{k-1} R$ (because $x_{k+1} \equiv x_k$ modulo $\pi^k R$).

Define $y = (y_{k+1} + \pi^k R)_{k \geq 2}$; then we have $y \in \hat{R}$

by this last property, and furthermore

$$\hat{\pi} y = (\pi R, \pi y_3 + \pi^2 R, \dots)$$

with $\pi y_3 + \pi^2 R = x_3 \mod \pi^2 R = x_2, \dots,$

which means that $\hat{\pi} y = x$.

Once we know that $(\hat{R}, \hat{v})$ is a valuation ring, it

is clearly a normalized DVR with uniformizer $\hat{\pi}$.

(3) The map $i \begin{cases} R \longrightarrow \hat{R} \\ x \longmapsto (x + \pi^h R)_{h \geq 1} \end{cases}$ is clearly a ring morphism. It is injective because $\ker(i) = \bigcap_{h \geq 1} \pi^h R = \{0\}$, and it is isometric because $\hat{v}(i(x)) = v(x)$ (the highest power of π that divides x in R) for all $x \in R$.

To show that $i(R) \subset \hat{R}$ is dense we take $x = (x_h)_{h \geq 1} \in \hat{R}$; for $m \geq 1$ fixed, let $y \in R$ be such that $y \equiv x_m \bmod \pi^m R$.

Then be definition we get

$$\hat{v}(x - i(y)) \geq m$$

(because $x_h - y \equiv 0 \bmod \pi^h R$ if $h \leq m$) so

$$d_v(x, i(y)) \leq 2^{-m}.$$

Since m is arbitrary we get elements of $i(R)$ approximating x arbitrarily closely.

(4) Now we prove that $\hat{R}$ is complete with

the metric $d_{\hat{v}}$.

For $k \geq 1$, we denote by $f_k : \hat{R} \longrightarrow R/\pi^k R$ the k-th coordinate projection. Note that if x, y are in $\hat{R}$, then $f_k(x) = f_k(y)$ if $\hat{v}(x-y) \geq k$. We consider then a Cauchy sequence $(x_n)_{n \geq 1}$ with $x_n \in \hat{R}$. Fix some $k \geq 1$. Since there exists n_0 such that $\hat{v}(x_n - x_m) \geq k$ if $n, m \geq n_0$ (because this means $\|x_n - x_m\|_{\hat{v}} \leq 2^{-k}$), we deduce that $f_k(x_n)$ is constant for $n \geq n_0$. Let y_k be this constant value. Then $y = (y_k)_{k \geq 1}$ is an element of $\hat{R}$ (because $f_{k+1}(x_n) \equiv f_k(x_n) \mod \pi^k R$, hence taking n large, $y_{k+1} \equiv y_k \mod \pi^k R$), and we have $x_n \longrightarrow y$ in $\hat{R}$:

$$\hat{v}(x_n - y) \geq k \quad \text{as soon as} \quad n \geq n_0$$

such that $f_k(y) = f_k(n)$.

(4) The fraction field $\mathrm{Frac}(\hat{R})$ is isomorphic

to $\hat{R}\left[\frac{1}{\hat{\pi}}\right]$ (This is a general fact for any DVR and uniformizer: $\frac{a}{b} \in \mathrm{Frac}(\hat{R})$ can be written $\frac{\hat{\pi}^{\hat{v}(a)} u}{\hat{\pi}^{\hat{v}(b)} v} = \hat{\pi}^{\hat{v}(a/b)} uv^{-1}$, with $uv^{-1} \in \hat{R}^*$)

If (x_n) is a Cauchy sequence in $\hat{K} = \mathrm{Frac}(\hat{R})$, then the sequence $(\hat{v}(x_n))$ is bounded from below: $\hat{v}(x_n) = \hat{v}(x_{n_0} + x_n - x_{n_0})$ for $n, n_0 \geq 1$, and if n_0 is chosen so that $\hat{v}(x_n - x_{n_0}) \geq 1$ if $n \geq n_0$, then we get

$$\hat{v}(x_n) \geq \min(\hat{v}(x_{n_0}), 1)$$

for $n \geq n_0$.

Let $v \in \mathbb{Z}$ be such that $\hat{v}(x_n) \geq v$ for all n. Then $y_n = x_n \hat{\pi}^{-v} \in \hat{R}$ and

$$\|y_n - y_m\|_{\hat{v}} = \|x_n - x_m\|_{\hat{v}} \, 2^{-v}$$

so (y_n) is also a Cauchy sequence, and therefore converges by (3), say to $y \in \hat{R}$. It follows that $x_n \longrightarrow y\hat{\pi}^v \in \hat{K}$. □

Definition. A complete DVR (R, v) is a DVR s.t. R is complete for the metric defined by v.

[In this case, $i(R) \subset \hat{R}$ is closed (because if $x_n = i(y_n)$ converges in $\hat{R}$, it is a Cauchy sequence in $\hat{R}$, so (y_n) is one in R because i is isometric; so y_n converges to some $y \in R$ and $i(y_n) \longrightarrow i(y)$); hence $i(R) \subset \hat{R}$ being closed and dense is equal to $\hat{R}$, so i is an isomorphism.]

Example. The properties of a complete DVR can be quite different from those of $\mathbb{R}$ or $\mathbb{C}$.

For instance, if (R, v) is a complete DVR, then a series $\sum_{n \geq 1} a_n$ with $a_n \in R$ converges if and only if $a_n \longrightarrow 0$ as $n \longrightarrow +\infty$. Indeed, with $s_N = \sum_{n=1}^{N} a_n$, we get $\| s_M - s_N \|_v \leq \max_{N \leq n \leq M} \|a_n\|_v$, by the non-archimedean triangle inequality, which shows that (s_N) is a Cauchy sequence, hence converges.

Example - Let p be a prime number, and let v_p be the p-adic valuation on $\mathbb{Z}$; the completion of the corresponding DVR R is denoted $\mathbb{Z}_p$ (if there is no risk of confusion...), and called the ring of p-adic integers. Its fraction field is denoted $\mathbb{Q}_p$, and called the field of p-adic numbers. It is the completion of $\mathbb{Q}$ with respect to the metric defined by v_p. (Indeed, $\mathbb{Z}$ itself is dense in $\mathbb{Z}_p$: to see this it is enough to observe that $R/p^k R$ is isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$ and repeat the proof that $i(R)$ is dense in $\mathbb{Z}_p$ with $i(\mathbb{Z})$ instead.)

Note that by definition we have

$$\mathbb{Z}_p \subset \prod_{k \geq 1} \mathbb{Z}/p^k\mathbb{Z} = X$$

and $\mathbb{Z}_p$ is closed when the product is given the product topology of the discrete topologies on the finite sets $\mathbb{Z}/p^k\mathbb{Z}$ (because the maps

$f_m : X \to \mathbb{Z}/p^m\mathbb{Z}$ and $g_m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^{m-1}\mathbb{Z}$

$(x_k) \mapsto x_m$ $\quad x \longmapsto x \bmod p^{m-1}$

are continuous, so

$$\mathbb{Z}_p = \bigcap_{m \geq 2} \{ x \in X \mid g_m(f_m(x)) = f_{m-1}(x) \}$$

is an intersection of closed sets). Since X is compact by Tychonov's Theorem, it follows that $\mathbb{Z}_p$ is also compact.

On the other hand, $\mathbb{Q}_p$ is not compact, but it is <u>locally compact</u> : indeed the sets

$$B_k = \{ x \in \mathbb{Q}_p \mid v(x) \geq k \} = p^k \mathbb{Z}_p$$

form a basis of compact neighborhoods of 0 in $\mathbb{Q}_p$ (compact because they are homeomorphic to $\mathbb{Z}_p$).

Note that these neighborhoods have again very unusual features in comparison with intervals in $\mathbb{R}$ for instance :

(i) each of these is a subgroup of $\mathbb{Q}_p$ (for addition)

(ii) besides being compact, these are also open : indeed, we have also

$$B_k = \left\{ x \in \mathbb{Q}_p \;\middle|\; \|x\|_{v_p} < 2^{-k+\frac{1}{2}} \right\}$$

since the p-adic valuation is discrete, and this is the inverse image by the continuous map $\|\cdot\|_{v_p} : \mathbb{Q}_p \longrightarrow [0, +\infty[$ of the open set $[0, 2^{-k+1/2}[$.

7 - Hensel's Lemma

We will now describe a very general and useful tool, Hensel's Lemma, which gives a general way to construct solutions of certain polynomial equations in complete DVRs.

Theorem - Let (R, v) be a complete DVR, π a uniformizer.

Let $f \in R[X]$ be a non-zero polynomial.

Let $k \geq 1$ and $x_1 \in R$ be such that

$$v(f(x_1)) \geq 1 \quad , \qquad v(f'(x_1)) = 0 .$$

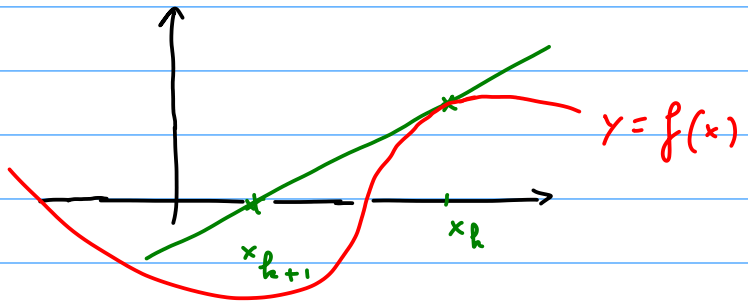
Then there exists a unique $y \in R$ such that

$$v(y - x_1) \geq 1 \quad \text{and} \quad f(y) = 0.$$

(Note: $v(f(x_1)) \geq 1$ means $f(x_1) \equiv 0 \bmod \pi R$ so the statement means that if $f(x_1)$ is "close enough" to zero, then there is an actual root of f in R "close" to x_1)

(In fact, $x = \lim_{n \to \infty} x_n$ where $(x_n)_{n \geq 0}$ is defined by $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.)

(In other words, by the Newton algorithm!)



Proof - We will construct $y = (y_n) \in R$ with $y_1 = x_1$ such that $f(y) = 0$. We determine y_{n+1}, assuming that y_n is known, as follows: we look for $y_{n+1} = \tilde{y}_n + \alpha \pi^n + \bar{\pi}^{n+1} R$, where $\tilde{y}_n \bmod \pi^n = y_n$, $\alpha \in R$, so that

$$f(y_{n+1}) = 0 \mod \pi^{n+1} R.$$

Doing this by induction will construct y, and if the choice of y_{n+1} is unique, then y is unique.

The condition above is that

$$f(\tilde{y}_n + \alpha \pi^n) = 0 \mod \pi^{n+1} R$$

$$\| $$

$$f(\tilde{y}_n) + \alpha \pi^n f'(\tilde{y}_n) \mod \pi^{n+1} R.$$

By induction, $f(\tilde{y}_n) = \beta \pi^n$ for some $\beta \in R$, so the condition becomes

$$\beta + \alpha f'(\tilde{y}_n) = 0 \mod \pi R.$$

We have also $f'(\tilde{y}_n) = f'(y_1) \neq 0 \mod \pi R$, so there is indeed a unique suitable choice of α (modulo πR), namely $\alpha \equiv -\frac{\beta}{f(y_1)} \mod \pi R$.

□

Example. Let $R = \mathbb{Z}_p$ be the ring of p-adic integers and $f = X^2 + d$ for some $d \in \mathbb{Z}$. Then $f' = 2X$. So there is a root of f

in $\mathbb{Z}_p$ provided $-d$ is a square in $\mathbb{Z}/p\mathbb{Z}$ (the residue field), $p \neq 2$, and $p \nmid d$ [so that if $x^2 \equiv -d \bmod p$, then $2x \not\equiv 0$].

(For $p = 2$, one can prove a similar statement by refining Hensel's Lemma, starting with an approximation mod p^2, etc...)

B. The theorem of Skolem - Mahler - Lerch

This was stated in Chapter I:

Theorem. Let $(u_n)_{n \geq 1}$ be a linear recurrence sequence in $\mathbb{Z}$, i.e. for some $k \geq 1$ and integers a_i, we have $u_{n+k} = a_1 u_{n+k-1} + \dots + a_k u_n$ for $n \geq 1$. Then there exist $q \geq 1$ and α_j, β_j in $\mathbb{Z}$ for $1 \leq j \leq q$ such that

$$u_n = 0 \iff \exists\, j, m, \quad n = \alpha_j + m\beta_j$$

(The set of n s.t. $u_n = 0$ is a finite union of arithmetic progressions.)

We will sketch a proof which relies on the use of p-adic numbers for some well-chosen prime p.

Step 1 - There exists a matrix $A \in M_k(\mathbb{Z})$ with $\det(A) \neq 0$, and $v_0 \in \mathbb{Z}^k$, $w_0 \in \mathbb{Z}^k$ s.t.

$$u_n = \langle A^n v_0, w_0 \rangle \qquad \forall n.$$

(This is elementary ; for example

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_{n+1} + u_{n+2} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_{n+2} \end{pmatrix}$$

for the Fibonacci sequence.)

Step 2 - There exists a prime number $p \geq 3$ and an integer $m \geq 1$ such that

$$\begin{cases} A \bmod p \in GL_k(\mathbb{Z}/p\mathbb{Z}) \\ A^m \equiv \mathrm{Id} \bmod p \end{cases}$$

(Indeed, take p such that $p \nmid \det(A)$, then note that $A \bmod p$ has finite order m in the finite group $GL_k(\mathbb{Z}/p\mathbb{Z})$.)

Step 3 - Fix an integer r with $0 \leq r < m$.

Define f on $\mathbb{N}$ by $f(a) = u_{ma+r}$.

Claim: **either** $f = 0$ or f has only finitely many zeros.

This claim implies the Theorem.

To prove it, we need a key lemma:

Lemma - There exist polynomials $q_j \in \mathbb{Z}_p[X]$ for $j \geq 0$ such that $f(a)$ is given for all $a \geq 0$ by the series

$$\sum_{j \geq 0} q_j(a)\, p^j$$

which converges in $\mathbb{Z}_p$.

($\mathbb{Z}_p$: p-adic integers)

Proof - Write $A^m = 1_k + pB$. Then (unit matrix)

$$f(a) = \langle A^{ma+r} v_0, w_0 \rangle$$

$$= \langle A^{ma} \tilde{v}_0, w_0 \rangle, \quad \tilde{v}_0 = A^r v_0$$

$$= \sum_{j=0}^{a} \binom{a}{j} p^j \langle B^j \tilde{v}_0, w_0 \rangle .$$

Note that $\binom{a}{j} = \dfrac{a(a-1)\cdots(a-j+1)}{j!}$

so

$$p^j \binom{a}{j} = \frac{p^j}{j!}\, a \cdots (a-j+1)$$

$$= \frac{p^j}{j!}\, \tilde{q}_j(a)$$

where $\tilde{q}_j \in \mathbb{Z}[X]$.

Moreover for all $j \geq 0$

$$v_p(j!) = \left\lfloor \frac{j}{p} \right\rfloor + \cdots + \left\lfloor \frac{j}{p^m} \right\rfloor + \cdots$$

$$\leq \frac{j}{p-1} \leq \frac{j}{2} \quad \text{since } p \geq 3,$$

so that $\dfrac{p^j}{j!} \xrightarrow[j \to +\infty]{} 0$ in $\mathbb{Z}_p$.

So the series

$$\sum_{j \geq 0} \binom{a}{j} p^j < B^j \tilde{v}_0, w_0 >$$

$$= \sum_{j \geq 0} \underbrace{\tilde{q}_j(a)}_{\in \mathbb{Z}} \underbrace{\frac{p^j}{j!}}_{\to 0} \underbrace{< B^j \tilde{v}_0, w_0 >}_{\in \mathbb{Z}}$$

converges in $\mathbb{Z}_p$ for all $a \in \mathbb{Z}$; the RHS makes sense for all $a \in \mathbb{Z}_p$ (since $\tilde{q}_j(a) \in \mathbb{Z}_p$ then) and the resulting $\tilde{f} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ coincides

with f for $a \in \mathbb{N}$. Putting

$$p_j(X) = \langle B^j \tilde{v}_0, w_0 \rangle \frac{\tilde{q}_j(X)}{j!} \in \mathbb{Z}_p[X]$$

we obtain the lemma.

□

We now prove the Claim using this Lemma: writing p_j as a polynomial and exchanging the sums (which is more easily justified than in classical analysis) we see that $\tilde{f}$ is in fact a power series

$$\tilde{f}(a) = \sum_{n \geq 0} \alpha_n a^n$$

where $\alpha_n \in \mathbb{Z}_p$, convergent for $a \in \mathbb{Z}_p$. Like classical power series we have $\tilde{f} = 0$ if and only if $\alpha_n = 0$ for all n, and if this is not the case, the zeros of $\tilde{f}$ in $\mathbb{Z}_p$ form a discrete set. But then this set of zeros is discrete and closed, hence compact (since

$\mathbb{Z}_p$ itself is compact) so the set of zeros of $\tilde{f}$ in $\mathbb{Z}_p$ is finite, and so is the set of zeros of f in $\mathbb{N}$.