

NOTES ON FILTRATIONS, TOPOLOGIES, AND COMPLETIONS

J.P. MAY

CONTENTS

1.	Filtered groups	1
2.	Filtered rings and modules	2
3.	The Artin–Rees Lemma and Krull intersection theorem	3
4.	I -adic completion	4
5.	Faithfully flat R -modules	5
6.	Zariski rings	7
7.	The I -adic metric on R	7
8.	Hensel’s lemma	8

1. FILTERED GROUPS

1. Let G be a group with a decreasing filtration by normal subgroups G_i . Then G is a topological group. The G_i form a fundamental system of neighborhoods of the identity. The open subsets are the arbitrary unions of finite intersections of cosets gG_i .

2. The following are equivalent.

- (i) G is Hausdorff.
- (ii) Points in G are closed.
- (iii) The G_i intersect in $\{e\}$.

Of course, (i) implies (ii) by general topology. For (ii) implies (i), the diagonal in $G \times G$ is $\mu^{-1}(e)$, where $\mu(g, h) = gh^{-1}$. Since $G - G_i$ is the union of the cosets gG_i with $g \notin G_i$, $G - G_i$ is open, hence $G - G_i$ is both open and closed, hence so is G_i . Now (iii) clearly implies (ii). If x is in all G_i and is not e , then there are no open neighborhoods separating e and x , so G is not Hausdorff.

3. If $H \supset G_i$, then $H - G_i$ is open since it is the union of the cosets hG_i , $h \in H - G_i$ and, similarly, H is also closed.

4. $G/\cap G_i$ is the associated Hausdorff group of G .

5. Consider the canonical map $\gamma: G \rightarrow \lim G/G_i$, obtained from the quotient homomorphisms $\gamma_i: G \rightarrow G/G_i$. Give the target the inverse limit topology, where the G/G_i are discrete. Then γ is continuous since $\gamma_i^{-1}(eG_i) = G_i$. If γ is a bijection, then it is a homeomorphism. Indeed, the G_i then give a fundamental system of neighborhoods of the identity in both. We say that G is complete when this holds.

6. Define the completion of G to be $\hat{G} = \lim G/G_i$; it is more accurate to view the map $\gamma: G \rightarrow \hat{G}$ as the completion of G . Let \hat{G}_i be the kernel of $\hat{G} \rightarrow G/G_i$. This gives \hat{G} a decreasing filtration, and the topology on \hat{G} is the same as the topology associated to this filtration. Moreover, $G/G_n \cong \hat{G}/\hat{G}_n$.

7. Two filtrations of G give the same topology if for each m and n there exist p and q such that $G_m \subset G'_p$ and $G'_n \subset G_q$. By cofinality, the completions are isomorphic as topological groups (homeomorphic via an isomorphism of groups).

2. FILTERED RINGS AND MODULES

Let R be a commutative ring and M an R -module. We consider decreasing filtrations $R = R_0 \supset R_1 \supset R_2 \supset \cdots$ by ideals such that $R_i \cdot R_j \subset R_{i+j}$. Similarly, we consider decreasing filtrations $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ by sub R -modules such that $R_i \cdot M_j \subset M_{i+j}$. In favorable cases $\bigcap R_i = \{0\}$ and $\bigcap M_i = \{0\}$. The notations $F_i R = R_i$ and $F_i M = M_i$ are frequently used. In the most important example, we take an ideal I of R and define $R_i = I^i$ and $M_i = I^i M$. These are called I -adic filtrations.

We can apply the constructions of the previous section to the underlying filtered Abelian groups of R and M . The completion \hat{R} inherits a multiplication from R , and the completion \hat{M} becomes an \hat{R} -module. We are interested in understanding the exactness properties of these constructions. We start in the general case in this section and specialize to I -adic completions in the next.

We start over with a filtered R -module M , with no filtration given on $R = R_0$, so that each M_i is an R -module. Of course each M_i is open and closed in the resulting “linear topology” on M . Let N be a sub R -module of M and let $P = M/N$. Then N has the filtration given by $N_i = N \cap M_i$, P has the filtration given by letting P_i be the image of M_i , and N and P have associated linear topologies.

1. The subspace topology on N coincides with the linear topology. Indeed, a subset $X \subset N$ is open in the subspace topology iff $X = N \cap U$ for some open subset U of M , while X is open in the linear topology iff X is a union of finite intersections of subsets of the form $x + N_i = x + N \cap M_i$, $x \in N$. Here U is a union of finite intersections of the form $y + M_i$, but if $N \cap (y + M_i)$ is non-empty, then $y + M_i = x + M_i$ for some $x \in N$.

2. The closure \bar{N} of N in M is given by $\bar{N} = \bigcap_i (N + M_i)$. Indeed, $x \in \bar{N}$ iff $(x + M_i) \cap N \neq \emptyset$ for all i , and that holds if and only if $x \in N + M_i$ for all i . Therefore N is closed in M iff $\bigcap (N + M_n) = N$, and this holds iff $\bigcap P_i = 0$, that is, iff P is Hausdorff in the linear topology.

3. The quotient topology on P coincides with the linear topology. Indeed, let $X \subset P$. Then X is open in the quotient topology iff the inverse image, Y say, of X in M is open. This means that if $y \in Y$ then $y + M_i \subset Y$ for some i . Reducing mod N , this means that if $x \in X$, then $x + P_i \subset X$ for some i , which means that X is open in the linear topology on P .

4. Since $P/P_i \cong M/N + M_i$, we have the short exact sequences

$$0 \longrightarrow N/N \cap M_i \longrightarrow M/M_i \longrightarrow P/P_i \longrightarrow 0.$$

On passage to limits, there results a short exact sequence

$$0 \longrightarrow \hat{N} \longrightarrow \hat{M} \longrightarrow \hat{P} \longrightarrow 0.$$

That is, $\widehat{M/N} \cong \hat{M}/\hat{N}$. Here \hat{N} is the closure of the image of N in \hat{M} . Exactness at the left is a general fact on inverse sequences. Exactness at the right uses that the maps in our inverse systems are epimorphisms. In detail, let $(p_j) \in \hat{P}$. Inductively, suppose chosen $m_i, i < j$, such that $m_i \rightarrow p_i$ and $m_i \rightarrow m_{i-1}$ for each i . Choose m'_j that maps to p_j . Then $m'_j - m_{j-1}$ is in $N + M_{j-1}$, say $m'_j - m_{j-1} = n + m$.

Let $m_j = m'_j - n = m_{j-1} + m$. Inductively, this gives an element (m_j) of \hat{M} that maps to (p_j) .

3. THE ARTIN–REES LEMMA AND KRULL INTERSECTION THEOREM

Let I be a proper ideal in R and $N \subset M$ be R -modules. Filtering M by the $I^i M$, we obtain two filtrations on N , namely the I -adic filtration given by the $I^i N$ and the submodule filtration given by the $N \cap I^i M$. Clearly $I^i N \subset N \cap I^i M$. The opposite inclusion fails, but the two linear topologies are sometimes the same. Let R be Noetherian and M be finitely generated throughout this section. Then we have the following result.

Lemma 3.1 (Artin–Rees). *There is an m such that*

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

and therefore $N \cap I^n M \subset I^{n-m} N$ for all $n > m$.

Proof. Define a graded ring $B_I(R) = R \oplus I \oplus I^2 \oplus \cdots$; it is called the Rees ring of (R, I) . Think of $B_I(R)$ as $R[It] \subset R[t]$ for an indeterminate t . Write $E_I^0 R$ (or $gr_I(R)$) for the associated graded ring of R with respect to the I -adic filtration, that is, $\bigoplus_{i \geq 0} I^i / I^{i+1}$. Observe that $B_I(R) / I B_I(R) \cong E_I^0 R$. Thus the construction replaces the associated graded by a simple quotient. Let $M_* = \{M_i\}$ be any decreasing I -filtration of M , meaning that $IM_i \subset M_{i+1}$. Say that the I -filtration is I -stable if $IM_n = M_{n+1}$ for all sufficiently large n . The filtration $\{I^i M\}$ is certainly I -stable, and the claim is that the filtration $\{N_i = N \cap I^i M\}$ is I -stable. Define $B(M_*) = M \oplus M_1 \oplus M_2 \oplus \cdots$ and observe that $B(M_*)$ is a graded $B_I(R)$ -module. The second of the following two lemmas is a generalized version of the result we are after. \square

Lemma 3.2. *The $B_I(R)$ -module $B(M_*)$ is finitely generated iff the I -filtration M_* is I -stable.*

Proof. Suppose that $B(M_*)$ is finitely generated. Its generators lie in the first m terms for some m . Replace the generators by their homogeneous components (or work homogeneously from the start). These components are still finite in number and still generate $B(M_*)$. Thus $B(M_*)$ is generated by the elements of the M_i for $i \leq m$. This implies that $M_m \oplus M_{m+1} \oplus \cdots$ is generated as a $B_I(R)$ -module by M_m . This means that $M_{i+m} = I^i M_m$ for $i \geq 0$ or, equivalently, that the filtration is I -stable. Conversely, if $M_{i+m} = I^i M_m$ for some m and all $i \geq 0$, then $B(M_*)$ is generated by the union of the sets of generators of the M_i for $i \leq m$, which is a finite set. \square

Lemma 3.3. *Let M_* be any I -stable filtration of M , such as $\{I^i M\}$, and let $N_i = N \cap M_i$. Then N_* is an I -stable filtration of N .*

Proof. Clearly $B(N_*)$ is a sub $B_I(R)$ -module of $B(M_*)$. Since M_* is I -stable, $B(M_*)$ is finitely generated. Since I is finitely generated, $B_I(R)$ is finitely generated as an R -algebra. Therefore, by the Hilbert basis theorem, $B_I(R)$ is a Noetherian ring. But then $B(N_*)$ is finitely generated and therefore N_* is I -stable. \square

Corollary 3.4 (Krull intersection theorem). *Let $N = \bigcap I^i M$. Then there exists $r \in R$ such that $1 - r$ is in I and $rN = 0$. If $I \subset \sqrt{R}$, then $N = 0$.*

Proof. By the Artin-Rees theorem and $N \subset I^m M$, there exists m such that

$$N = N \cap I^{m+1} M = I(N \cap I^m M) = IN.$$

The existence of r is now either a standard lemma in the proof of Nakayama's lemma (which says that $N = 0$ if $I \subset \sqrt{R}$) or is sometimes itself referred to as Nakayama's lemma. One proof is by induction on the number of generators of modules N such that $IN = N$. The last statement follows since r is a unit if $I \subset \sqrt{R}$. \square

4. I -ADIC COMPLETION

Let I be a proper ideal of a commutative ring R and let M be an R -module. We have the completion $\gamma: R \rightarrow \hat{R}_I = \lim R/I^i$, which is a continuous homomorphism of topological rings. We say that R is complete at I if γ is an isomorphism. We also have the completion $\gamma: M \rightarrow \hat{M}_I = \lim M/I^i M$, which is a continuous homomorphism of topological R -modules. Let $\hat{I} = \{(r_i) | r_0 = 0\}$. Then \hat{I} is an ideal of \hat{R}_I such that $\hat{I}^n = \{(r_i) | r_i = 0 \text{ if } i < n\}$. The associated graded rings $E_I^0 R$ and $E_I^0 \hat{R}$ are the same. The Artin-Rees lemma gives the following fundamental result.

Lemma 4.1. *If R is Noetherian, then completion is an exact functor on the category of finitely generated R -modules. Therefore \hat{R}_I is a flat R -module.*

Algebraic topologists must often work with rings that are not Noetherian and modules that are not finitely generated even when R is Noetherian. For them, the "right" notion of completion is not I -adic completion, but rather its zeroth left derived functor (and its first left derived functor is also relevant).

Lemma 4.2. *Let \mathfrak{m} be a maximal ideal of R . Then $\hat{R}_{\mathfrak{m}}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$, and $R/\mathfrak{m} = \hat{R}_{\mathfrak{m}}/\hat{\mathfrak{m}}$. The completion $R \rightarrow \hat{R}_{\mathfrak{m}}$ is the composite of the localization $R \rightarrow R_{\mathfrak{m}}$ and the completion $R_{\mathfrak{m}} \rightarrow \hat{R}_{\mathfrak{m}}$.*

Proof. We must show that an element (r_i) of \hat{R}_I that is not in $\hat{\mathfrak{m}}$ is a unit. Now $(r_i) \notin \hat{\mathfrak{m}}$ if and only if $r_0 \neq 0$ in R/\mathfrak{m} . Since r_i maps to r_0 under $R/\mathfrak{m}^i \rightarrow R/\mathfrak{m}$, r_i is not in $\mathfrak{m}R/\mathfrak{m}^i$, so is a unit in R/\mathfrak{m}^i . The sequence (r_i^{-1}) is $(r_i)^{-1}$ in $\hat{R}_{\mathfrak{m}}$. \square

A complete local ring R is a Noetherian local ring which is complete at its maximal ideal \mathfrak{m} . Such rings are central to number theory and algebraic geometry.

Example 4.3. The p -adic integers $\hat{\mathbb{Z}}_{(p)}$ are usually denoted \mathbb{Z}_p (or sometimes $\hat{\mathbb{Z}}_p$). They can be represented in terms of "infinite p -adic expansions" $\sum a_i p^i$, where $0 \leq a_i < p$.

Example 4.4. The completion of the polynomial ring $R[x_1, \dots, x_n]$ at the ideal $I = (x_1, \dots, x_n)$ is isomorphic to the power series ring $R[[x_1, \dots, x_n]]$. Explicitly, send a formal power series f to the element $(f \bmod I^i)$ of the completion. For the inverse, consider an element (f_i) of the completion. Here f_i can be represented $(\bmod I^i)$ as a polynomial of degree less than i in the x_q , and then $f_i = f_{i+1}$ plus terms of degree $i+1$. The formal power series $f_0 + (f_1 - f_0) + (f_2 - f_1) + \dots$ gives the corresponding element of the power series ring.

It is left as an exercise to prove that if R is I -adically complete, then I is contained in the radical of R . If M is I -adically complete, then it is an \hat{R}_I -module and therefore multiplication by $1 + a$, $a \in I$ is an automorphism of M .

It is also left as an exercise to prove that if $I = (a_1, \dots, a_n)$ is an ideal in a Noetherian ring R , then \hat{R}_I is isomorphic to

$$\hat{R}_I \cong R[[x_1, \dots, x_n]]/(x_1 - a_1, \dots, x_n - a_n).$$

This has the following basic consequence.

Corollary 4.5. *If R is Noetherian, then \hat{R}_I is Noetherian.*

One way to work the exercise just cited is to use the following result, which shows that ideal theory passes nicely to completions.

Proposition 4.6. *Let I and J be ideals in a commutative Noetherian ring R and let M be a finitely generated R -module. Then*

$$(\widehat{JM})_I = J \cdot \widehat{M}_I \quad \text{and} \quad (\widehat{M/JM})_I \cong \widehat{M}_I / J\widehat{M}_I.$$

Moreover, $(\widehat{JM})_I$ is the closure of JM in \widehat{M}_I .

Proof. By Artin–Rees, the short exact sequence

$$0 \longrightarrow JM \longrightarrow M \longrightarrow M/JM \longrightarrow 0$$

gives an exact sequence

$$0 \longrightarrow (\widehat{JM})_I \longrightarrow \widehat{M}_I \longrightarrow (\widehat{M/JM})_I \longrightarrow 0$$

on passage to I -adic completion, and this implies that $(\widehat{JM})_I$ is the closure of JM in \widehat{M}_I . Certainly $J \cdot \widehat{M}_I \subset (\widehat{JM})_I$. Let $J = (a_1, \dots, a_r)$ and define $\phi: M^r \rightarrow M$ by $\phi(m_1, \dots, m_r) = \sum a_i m_i$. The image of ϕ is JM , so we have an exact sequence

$$M^r \xrightarrow{\phi} M \xrightarrow{\pi} M/JM \longrightarrow 0.$$

On passage to limits, there results an exact sequence

$$(\widehat{M}_I)^r = (\widehat{M^r})_I \xrightarrow{\hat{\phi}} \widehat{M}_I \xrightarrow{\hat{\pi}} (\widehat{M/JM})_I \longrightarrow 0.$$

Since the kernel of $\hat{\pi}$ must be $(\widehat{JM})_I$, this gives $(\widehat{M/JM})_I \cong \widehat{M}_I / (\widehat{JM})_I$. Here again, $\hat{\phi}(m_1, \dots, m_r) = \sum a_i m_i$, where now $m_i \in \widehat{M}_I$. The image of $\hat{\phi}$ is $J \cdot \widehat{M}_I$, and this is equal to the kernel, $J\widehat{M}_I$, of $\hat{\pi}$. \square

Corollary 4.7. *Let \widehat{M}_i denote the kernel of the projection $\widehat{M}_I \rightarrow M/I^i M$. Then $\widehat{M}_i = I^i \cdot \widehat{M}_I$. Thus the linear topology of \widehat{M}_I coincides with its I -adic topology as an R -module, which in turn coincides with its $I \cdot \hat{R}_I$ -adic topology as an \hat{R}_I -module.*

Proof. $M/I^i M = (\widehat{M/I^i M})_I$, and the kernel of $\widehat{M}_I \rightarrow (\widehat{M/I^i M})_I$ is $I^i \cdot \widehat{M}_I$ by the previous result. \square

5. FAITHFULLY FLAT R -MODULES

An R -module N is said to be *faithfully flat* if a sequence of R -modules is exact if and only if it becomes exact on tensoring with N . We shall relate this notion to completions. We record the following general result.

Proposition 5.1. *An R -module N is flat if and only if the canonical map*

$$I \otimes_R N \longrightarrow R \otimes_R N \cong N$$

is a monomorphism for all finitely generated ideals I , so that $I \otimes_R N \cong IN$.

Proof. The forward implication is clear. Assume the condition on ideals. Any ideal is the colimit of its finitely generated ideals, and tensoring with N commutes with colimits. We conclude that $I \otimes_R N \rightarrow N$ is a monomorphism for any ideal I . Let $M' \rightarrow M$ be a monomorphism. We must show that $M' \otimes_R N \rightarrow M \otimes_R N$ is a monomorphism. Clearly M is the colimit of the sums $M' + M''$, where $M'' \subset M$ is finitely generated. By induction on the number of generators and passage to colimits, it suffices to show the required monomorphism when $M = M' + Rx$ for some $x \in M$. Let $I = \{r \mid rx \in M'\}$. We then have a short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow R/I \longrightarrow 0.$$

Since we have a short exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

and since $I \otimes_R N \rightarrow R \otimes_R N$ is a monomorphism, we see that $\text{Tor}_1^R(R/I, N) = 0$. Therefore $M' \otimes_R N \rightarrow M \otimes_R N$ is a monomorphism. \square

The following result, together with Nakayama's lemma, shows that flat modules are often necessarily faithfully flat.

Proposition 5.2. *The following conditions on an R -module N are equivalent.*

- (i) N is faithfully flat.
- (ii) N is flat and $M \otimes_R N = 0$ implies $M = 0$.
- (iii) N is flat and $\mathfrak{m}N \neq N$ if \mathfrak{m} is a maximal ideal.

Proof. (i) \implies (ii): If $M \otimes_R N = 0$, then $0 \rightarrow M \rightarrow 0$ becomes exact after tensoring with N , hence is exact, and $M = 0$.

(ii) \implies (iii): $N/\mathfrak{m}N \cong R/\mathfrak{m} \otimes_R N$, so this is clear.

(iii) \implies (ii): Assume $M \otimes_R N = 0$ and $x \in M$ is non-zero. Then $Rx \cong R/I$, where I is the annihilator of x . Embed I in a maximal ideal \mathfrak{m} . Since $IN \subset \mathfrak{m}N \neq N$, $Rx \otimes_R N \cong N/IN \neq 0$. Since N is flat $Rx \otimes_R N \rightarrow M \otimes_R N$ is a monomorphism, which contradicts the assumption that $M \otimes_R N = 0$.

(ii) \implies (i): Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ be a sequence such that

$$M' \otimes_R N \xrightarrow{f \otimes \text{id}} M \otimes_R N \xrightarrow{g \otimes \text{id}} M'' \otimes_R N$$

is exact. Then, using that N is flat, $\text{Im}(g \circ f) \otimes_R N = 0$. Therefore $\text{Im}(g \circ f) = 0$ and $g \circ f = 0$. Let $H = \text{Ker}(g)/\text{Im}(f)$. Again, $H \otimes_R N = 0$, hence $H = 0$. \square

A ring homomorphism $f: R \rightarrow S$ is said to be faithfully flat if S is faithfully flat as an R -module.

Proposition 5.3. *Let $f: R \rightarrow S$ be a faithfully flat ring homomorphism.*

- (i) For any R -module M , extension of scalars

$$\text{id} \otimes f: M = M \otimes_R R \rightarrow M \otimes_R S$$

is a monomorphism. In particular, f is a monomorphism.

- (ii) Regard f as an inclusion. If I is an ideal in R , then $IS \cap R = I$.

Proof. For (i), let $x \in M$ be non-zero. The monomorphism $Rx \otimes_R S \rightarrow M \otimes_R S$ has image $(x \otimes 1)S$, hence $x \otimes 1$ is non-zero. To see (ii), apply (i) to $M = R/I$, noting that $M \otimes_R S \cong S/IS$. If $r \in R$ is not in I , then it is also not in IS . \square

6. ZARISKI RINGS

A pair (R, I) consisting of a commutative Noetherian ring R and an ideal $I \subset \sqrt{R}$ is called a *Zariski ring*. The interest of this notion comes from the following result.

Theorem 6.1. *The following conditions are equivalent for an ideal I in a commutative Noetherian ring R .*

- (i) $I \subset \sqrt{R}$.
- (ii) Every ideal of R is closed in the I -adic topology.
- (iii) \hat{R}_I is faithfully flat over R .

Proof. (i) \implies (ii): More generally, $N \subset M$ is closed for any submodule of a finitely generated R -module M since M/N is Hausdorff by the Krull intersection theorem and therefore $\{0\}$ is closed in M/N .

(ii) \implies (iii): It suffices to show that $\mathfrak{m}\hat{R}_I \neq \hat{R}_I$ for every maximal ideal \mathfrak{m} . Since $\{0\}$ is closed in R , $\cap I^i = 0$ and the completion $\gamma: R \rightarrow \hat{R}_I$ is a monomorphism. Since \mathfrak{m} is closed in R and $\mathfrak{m}\hat{R}_I$ is the closure of \mathfrak{m} in \hat{R}_I , $\mathfrak{m}\hat{R}_I \cap R = \mathfrak{m}$ and therefore $\mathfrak{m}\hat{R}_I \neq \hat{R}_I$.

(iii) \implies (ii): $\mathfrak{m}\hat{R}_I \neq \hat{R}_I$ for any maximal ideal \mathfrak{m} . Since \hat{R}_I is I -adically complete, \hat{I}_I is contained in the radical of \hat{R}_I . As in (i) \implies (ii), if N is a submodule of a finitely generated \hat{R}_I -module M , then N is closed in M . Since γ is continuous, $\mathfrak{m} = \mathfrak{m}\hat{R}_I \cap R$ is closed in R . If I is not contained in \mathfrak{m} , then $I^i + \mathfrak{m} = R$ for all $i > 0$, contradicting that \mathfrak{m} is closed in R . Therefore $I \subset \sqrt{R}$. \square

Consider a Noetherian local ring R with maximal ideal \mathfrak{m} . Obviously, $\mathfrak{m} = \sqrt{R}$. We have proven the following results. Recall that R is said to be complete if it is \mathfrak{m} -adically complete.

1. $\cap \mathfrak{m}^i = 0$.
2. If N is a submodule of a finitely generated R -module M , then N is closed in the \mathfrak{m} -adic topology. That is, $N = \cap(N + \mathfrak{m}^i N)$.
3. Let $\hat{R} = \hat{R}_{\mathfrak{m}}$. Then \hat{R} is faithfully flat over R , $R \subset \hat{R}$, and $I = I\hat{R} \cap R$ for any ideal I .
4. \hat{R} is a Noetherian local ring with maximal ideal $\mathfrak{m}\hat{R}$, and $\hat{R}/\mathfrak{m}^i \hat{R} \cong R/\mathfrak{m}^i$ for $i > 0$. In particular, R and \hat{R} have the same residue field.
5. If R is a complete local ring and I is a proper ideal, then R/I is a complete local ring.

 7. THE I -ADIC METRIC ON R

Let I be an ideal in R and define $d(x, y)$ to be $1/n$ if $x - y$ is in I^n and not in I^{n+1} and to be 0 if $x - y \in \cap I^n$. Then $d(x, y) = d(y, x)$ and

$$d(x, z) \leq \max(d(x, y), d(y, z)) \leq d(x, y) + d(y, z).$$

Thus d is a pseudo-metric on R , and it is a metric if $\cap I^n = 0$.

Any pseudo-metric space X is normal. If A and B are disjoint closed subset of X , let $U = \{x | d(A, x) < d(B, x)\}$ and $V = \{x | d(B, x) < d(A, x)\}$. Then U and V are disjoint open subsets that contain A and B . Of course, X need not be Hausdorff since points need not be closed.

We assume the reader knows what a Cauchy sequence is and what it means for two Cauchy sequences to be equivalent. We say that X is complete if every Cauchy sequence converges, and every Cauchy sequence then converges to a unique point

if X is Hausdorff. We define the completion of X to be the set of equivalence classes of Cauchy sequences with the induced metric topology, where $d((x_n), (y_n))$ is the limit of the $d(x_n, y_n)$. The completion $\gamma: X \rightarrow \hat{X}$ sends x to the constant sequence at x , and it is a continuous map with dense image.

Proposition 7.1. *The completion of R at I is canonically homeomorphic to its completion in the I -adic metric.*

Indeed, the metric topology is the same as the I -adic topology on R . More explicitly, an element (r_i) of $\lim R/I^i$ can be viewed as an equivalence class of Cauchy sequences in R .

8. HENSEL'S LEMMA

Here is one fundamental and beautiful reason to care about complete rings, and especially complete local rings.

Lemma 8.1 (Hensel's lemma). *Let R be an I -adically complete Noetherian ring and let $k = R/I$ be the residue ring. Use small letters for polynomials in $k[x]$ and capital letters for polynomials in $R[x]$. Let F be a polynomial in $R[x]$ that reduces mod I to a polynomial $f = gh$ in $k[x]$, where g and h are relatively prime and g is monic. Then there is a factorization $F = GH$ in $R[x]$ such that G and H reduce mod I to g and h and G is monic. If h is also monic, then H can be chosen to be monic and the resulting factorization is unique.*

Sketch Proof. Choose any polynomials G_1 and H_1 that reduce mod I to g and h , taking G_1 to be monic and taking $\deg(G_1) = \deg(g)$ and $\deg(H_1) = \deg(h)$. Proceeding inductively, suppose given G_n and H_n that reduce mod I^n to g and h , where G_n is monic, $\deg(G_n) = \deg(g)$ and $\deg(H_n) = \deg(h)$. Write $F - G_n H_n = \sum a_i J_i$, where $a_i \in I^n$ and $\deg(J_i) < \deg(F)$. Since $(g, h) = 1$, there are polynomials u_i and v_i such that $j_i = gu_i + hv_i$, and we can arrange that $\deg(u_i) < \deg(h)$ by replacing u_i by its remainder after division by h and adjusting v_i accordingly. Then $\deg(hv_i) = \deg(j_i - gu_i) < \deg(f)$ and therefore $\deg(v_i) < \deg(g)$. Choose U_i and V_i that reduce mod I to u_i and v_i , with $\deg(U_i) = \deg(u_i)$ and $\deg(V_i) = \deg(v_i)$. Set $G_{n+1} = G_n + \sum a_i V_i$ and $H_{n+1} = H_n + \sum a_i U_i$. A quick check shows that $F \equiv G_{n+1} H_{n+1} \pmod{I^{n+1}}$, G_{n+1} is monic, $\deg(G_{n+1}) = \deg(g)$ and $\deg(H_{n+1}) = \deg(h)$. Then (G_n) and (H_n) are Cauchy sequences (coefficient-wise) and we can pass to limits to obtain polynomials G and H as required. When h is monic, we can choose the H_n to be monic, and comparison shows that different choices of the sequences G_n and H_n give equivalent Cauchy sequences. \square

Corollary 8.2. *If $F \in R[x]$ and $a \in R$ are such that $F'(a)$ is a unit in R and $F(a) \equiv 0 \pmod{I}$, then there exists $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{I}$.*

Proof. Reducing mod I , $f(x) = (x - \bar{a})g(x)$. Since

$$\begin{aligned} f'(x) &= g(x) + (x - \bar{a})g'(x), \\ g(x) &\equiv f'(x) \equiv f'(\bar{a}) \pmod{(x - \bar{a})}. \end{aligned}$$

Since $f'(\bar{a})$ is a unit in k , $g(x)$ and $x - \bar{a}$ generate $k[x]$ and thus are relatively prime. Hensel's lemma gives $F(x) = (x - b)G(x)$, where G reduces to g and $x - b$ reduces to $x - \bar{a} \pmod{I}$. \square