

FILTERED RINGS AND MODULES. GRADINGS AND COMPLETIONS.

Let A be a ring, for simplicity assumed commutative. A *filtering*, or *filtration*, of an A module M means a descending sequence of submodules $M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots$, for integers $n \geq 0$.

For example, if $I \subset A$ is an ideal then there is the I -adic filtering $A \supset I \supset I^2 \supset \cdots$ by powers of I , and a corresponding I -adic filtering $M \supset IM \supset I^2M \supset \cdots$ of any A module.

In general, a filtering $M \supset M_n$ is called an I -filtering if $I^d M_n \subset M_{n+d}$ for all $d, n \geq 0$.

A *graded ring* A_* means a ring which is a direct sum $A_* = \bigoplus A_n$, $n \geq 0$, with $A_i A_j \subset A_{i+j}$ for all i, j . In particular, $1 \in A_0$, which is a ring.

An important example of a graded ring is the polynomial ring $A_* = k[x_1, \dots, x_n]$ over a ground ring k . We declare each x_j to have homogeneous degree 1, and then take A_n to be the (free) $k = A_0$ module spanned by homogeneous monomials of degree n in the x_j . An ideal J in the polynomial ring is said to be *homogeneous* if it is generated by homogeneous polynomials, that is, polynomials in the various A_n . Equivalently, each homogeneous summand of an element of J should belong to J . So $J = \bigoplus J_n$. The ring $A_*/J_* = \bigoplus A_n/J_n = k[x_1, \dots, x_n]/J$ is then also a graded ring. Such graded rings arising from homogeneous polynomial ideals are of basic importance in projective algebraic geometry.

A graded A_* module means a module $M_* = \bigoplus M_n$, with $A_i M_j \subset M_{i+j}$. For example, associated to the I -adic filtering of A there is a graded ring $A_* = A_*(I) = \bigoplus I^n$, where $I^0 = A$. For any A module M there is also a graded A_* module $M_* = M_*(I) = \bigoplus I^n M$. In fact, any I -filtering of an A module M gives rise to a graded A_* module $M_* = \bigoplus M_n$.

It is important to understand the Noetherian chain condition for graded rings and modules.

PROPOSITION 1. A graded ring A_* is Noetherian if and only if A_0 is Noetherian and A_* is finitely generated as an algebra over A_0 .

PROOF. The if direction is an immediate consequence of the Hilbert Basis Theorem, since all commutative rings finitely generated over a Noetherian ring are Noetherian.

For the only if direction, first observe that A_* Noetherian implies the ideal $A_*^+ = \bigoplus_{n>0} A_n$ is finitely generated. We may as well assume the ideal A_*^+ is generated over A_* by finitely many homogeneous elements $\{x_{d_j}\}$, that is elements of various A_{d_j} , $d_j > 0$, because we can replace any set of generators by the homogeneous summands of those generators. Now I claim that this finite list of homogeneous elements generates A_* as an algebra over A_0 . Namely, by

induction on n we see that the A_0 module A_n is spanned by monomials in the x_{dj} of total degree n .

For $n = 1$ this is trivial, the x_{1j} must span A_1 over A_0 . Then by hypothesis all elements of A_2 are sums of A_0 linear combinations of the x_{2j} and products of the x_{1k} by elements of A_1 . By the $n = 1$ case, these latter elements are A_0 linear combinations of the monomials $x_{1k}x_{1j}$. The induction continues routinely to A_3 and beyond.

We also observe $A_0 = A_*/A_*^+$, so A_* Noetherian implies A_0 Noetherian. This completes the proof of the only if direction of the proposition.

Next, we say that an I -filtering $M \supset M_n$ of an A module is I -stable if for some integer s and all $d \geq 0$ one has $I^d M_s = M_{d+s}$. Obviously the I -adic filtering $M_n = I^n M$ is I -stable.

In general one has $I^{d+s}M \subset I^d M_s \subset M_{d+s} \subset M_d$ for any I -filtering, and any s, d . An I -stable filtering also satisfies $M_{d+s} = I^d M_s \subset I^d M$ for some large s and all d .

For later purposes, when we turn to completions, we point out that the inclusions in the above paragraph imply that if we impose an I -adic topology on M as a topological abelian group by declaring a fundamental basis of neighborhoods of 0 to be the subgroups $I^k M$, then any I -stable filtration M_k of M defines the same topology. By this we mean that if fundamental neighborhoods of 0 are taken to be the subgroups M_k instead of the $I^k M$, then the topology doesn't change. A more algebraic consequence of the above inclusions for an I -stable filtration is that there is an isomorphism of inverse limits

$$\varprojlim \frac{M}{I^k M} \simeq \varprojlim \frac{M}{M_k}.$$

Of course it then also follows that any two I -stable filtrations of M define the same topology and the same inverse limit.

Another important property of I -stable filtrations is a connection with graded Noetherian modules.

PROPOSITION 2: Suppose A is a Noetherian ring and M is a finitely generated A module with an I -filtration M_n . Then M_* is a finite A_* module if and only if the filtration M_n is I -stable.

PROOF: First, A_* is Noetherian by Proposition 1, because the ideal I is finitely generated and clearly $I = A_1$ generates $A_* = \bigoplus I^n$ over $A = A_0$. If M_* is a finite A_* module then it is a Noetherian module. Consider the increasing chain of A_* submodules

$$L_{*k} = M \oplus M_1 \oplus \cdots \oplus M_k \oplus IM_k \oplus I^2 M_k \oplus \cdots.$$

The chain must stabilize, but the union over k of the L_{*k} is clearly M_* . Therefore some $L_{*s} = M_*$, which exactly says M_n is an I -stable filtration.

For the converse direction, assuming $M_{d+s} = I^d M_s$ for some s and all d , it is obvious that M_* is spanned over A_* by $M \oplus M_1 \oplus \cdots \oplus M_s$. Each of the A modules M_j is finitely generated, so M_* is a finite A_* module.

The proposition just proved allows an easy proof that with Noetherian hypotheses, an I -stable filtration on an A module M will contract to an I -stable filtration on any submodule $L \subset M$. It is rather difficult to see why this should be so, without the efficient use of graded Noetherian ring and module principles, including the use of the Hilbert Basis Theorem, that we organized above.

THEOREM (Artin-Rees): Suppose A is a Noetherian ring, M a finite A module with an I -stable filtration M_n . Suppose $L \subset M$ is a submodule and set $L_n = L \cap M_n$. Then L_n is an I -stable filtration.

PROOF: $IL_n \subset IL \cap IM_n \subset L \cap M_{n+1} = L_{n+1}$, so at least we have an I -filtration of L . But L_* is a submodule of the finite A_* module M_* . As seen above, A_* is Noetherian. Hence L_* is also a finite A_* module, and the I -filtration is stable by Proposition 2.

If we take $M_n = I^n M$, then we obtain the following version of the theorem.

PROPOSITION 3: Suppose A is a Noetherian ring, M a finite A module, $L \subset M$ a submodule. Then for some integer s we have $I^d(L \cap I^s M) = L \cap I^{d+s} M$ for all $d \geq 0$.

This formulation of Artin-Rees leads to some understanding of certain infinite intersections in A modules.

PROPOSITION 4: Suppose A is a Noetherian ring, $I \subset A$ an ideal, M a finite A module. Set $M' = \bigcap I^n M \subset M$. Then

$$IM' = M' = \{x \in M \mid (1+y)x = 0, \text{ some } y \in I\}.$$

In particular, if $I \subset \text{Jac}(A)$, the Jacobson radical, or if M is a faithful A module, then $\bigcap I^n M = (0)$.

As special cases, one concludes the intersection of all powers of the maximal ideal in a Noetherian local ring is (0) , and, by localizing, the intersection of all powers of any prime ideal in a Noetherian *domain* is (0) .

PROOF: First, $I^m M \cap M' = M'$ for any m . By Artin-Rees, for some s we have $IM' = I(I^s M \cap M') = I^{s+1} M \cap M' = M'$.

Certainly if $x = yx = y^2x = \cdots$ with $y \in I$ then $x \in \bigcap I^n M$. Conversely, M' is a finite module, so by the standard determinant trick or induction on the number of generators, if $IM' = M'$ then there is some $y \in I$ with $(1+y)M' = (0)$.

There is another important method of associating graded rings and modules to filtrations. If $I \subset A$ is an ideal, set $Gr_* A = Gr_* = \bigoplus I^n / I^{n+1}$. The products $I^n I^m \subset I^{n+m}$ yield a well-defined multiplication and ring structure on $Gr_* A$. Note now $Gr_0 = A/I$. We definitely ‘lose information’ passing from A to $Gr_* A$.

As an example, suppose A is the affine coordinate ring of an algebraic curve over an algebraically closed field k , and suppose $m \subset A$ is a maximal ideal corresponding to a point on the curve. It is easy to see that if we take $I = m$ above then $Gr_*A = Gr_*A_{(m)}$. Moreover, if m corresponds to a non-singular point then $Gr_*A_{(m)} \simeq k[t]$, a polynomial ring in one variable. Specifically, t is any generator of m/m^2 , which is the same as a generator of the principal ideal $m \subset A_{(m)}$. There is nothing special about curves here. If one begins with the affine coordinate ring of an irreducible variety of dimension r , and if one localizes at a maximal ideal corresponding to a non-singular point, then the associated graded ring Gr_* is a polynomial ring in r variables over k .

We can also form graded modules in this second manner. If M is an A module, set $Gr_*M = \bigoplus I^n M / I^{n+1} M$. More generally, given an I -filtration M_n of M , we can form $Gr_*M = \bigoplus M_n / M_{n+1}$. In both these situations, Gr_*M is a graded Gr_*A module.

In the same spirit as our previous propositions concerning Noetherian conditions, we record the following result.

PROPOSITION 5: Suppose A is a Noetherian ring, $I \subset A$ an ideal. Then Gr_*A is Noetherian. If M is a finite A module and M_n is a stable I -filtration, then Gr_*M is a finite Gr_*A module.

PROOF: Ideal I is finitely generated. If $\{x_i\}$ span $I/I^2 = Gr_1$ over $A/I = Gr_0$ then it is clear that Gr_*A is a quotient of the Noetherian ring $A/I[x_i]$. For the module statement, the I -stable hypothesis easily implies Gr_*M is generated over Gr_*A by a finite number of terms $\bigoplus_{j=0}^s M_j / M_{j+1}$. But each of these summands is a finite A/I module.

Now we will take up certain completions of rings and modules. Suppose M_n is a filtration of an A module M . We define a topology making M into a topological abelian group by declaring the M_n to be a fundamental system of neighborhoods of $0 \in M$. A fundamental system of neighborhoods of $x \in M$ is given by the cosets $x + M_n$. A basis for the open sets of the filtration topology will be all the cosets $y + M_n$, $y \in M, n \geq 0$. All we use here for the definition of the topology is the additive abelian group structure of M , the module structure will play a later role.

Since the M_n are additive subgroups of M , we see that $(x + M_n) \cap (y + M_n) \neq \emptyset$ if and only if $x - y \in M_n$. It follows that the topology is Hausdorff if and only if $\bigcap M_n = (0)$. It is also routine to check that addition and the map taking an element of M to its negative are continuous. So M is a topological abelian group. Two elements $x, y \in M$ are 'close' if $x - y \in M_n$ for 'large' n .

An example to keep in mind is $M = \mathbb{Z}$ with $M_n = (p^n)$ for some prime p . In this p -adic topology, integers are close if their difference is divisible by a high power of p . In fact, if A is any ring and $I \subset A$ is an ideal, there is an I -adic topology on A defined by the filtration I^n . One can verify that multiplication is also continuous, so A with the I -adic topology becomes a topological ring.

In terms of a filtration topology on M it is routine to define *Cauchy sequences* (x_k) where $x_k \in M$. Namely, for all n there should exist $k = k(n)$ so that $m, m' \geq k$ implies $x_m - x_{m'} \in M_n$. In particular, a null sequence (z_k) is a Cauchy sequence, where null sequence means $z_m \in M_n$ for all $m \geq \text{some } k(n)$. Sums and differences of Cauchy sequences are Cauchy. We then define \hat{M} to be the abelian group of equivalence classes of Cauchy sequences, where two sequences are equivalent if their difference is a null sequence. There is a group homomorphism $M \rightarrow \hat{M}$ that assigns to each $x \in M$ the constant sequence $(x_k = x), k \geq 0$. Note that a constant sequence (x) is a null sequence exactly when $x \in \bigcap M_n$. So when the topology on M is Hausdorff, the map $M \rightarrow \hat{M}$ is an embedding.

Following the language of analysis, we say that M is *complete* in a Hausdorff filtration topology if every Cauchy sequence (x_k) converges to some $x \in M$. This means $(x_k - x)$ is a null sequence. Given any filtration topology on M there is a *Hausdorff* filtration topology on \hat{M} . Namely \hat{M}_n consists of equivalence classes of Cauchy sequences (x_k) with $x_k \in M_n$ for all large k . The point is, $(x_k) \in \bigcap \hat{M}_n$ exactly when (x_k) is a null sequence, and null sequences represent $0 \in \hat{M}$.

PROPOSITION 6: If M_n is any filtration of M then \hat{M} is complete in the Hausdorff filtration topology \hat{M}_n .

PROOF: A standard argument works in which you consider a Cauchy sequence of Cauchy sequences and construct a limit Cauchy sequence by choosing a term sufficiently far out in each of the original sequences.

But another point of view proceeds by introducing the inverse limit

$$\varprojlim M/M_n \subset \prod M/M_n$$

consisting of all ‘coherent tuples’ (\bar{x}_n) , where $\bar{x}_{n+1} \mapsto \bar{x}_n$ under the obvious surjections $M/M_{n+1} \rightarrow M/M_n$.

It is relatively routine to define bijections $\hat{M} \leftrightarrow \varprojlim M/M_n$. Map a Cauchy sequence (x_k) to the tuple (\bar{y}_n) where \bar{y}_n is the stable class of $x_k \in M/M_n$ for large k . Given a coherent tuple (\bar{x}_n) , map it to the Cauchy sequence class (x_n) .

Under these bijections, it is easy to check that the filtration subgroup \hat{M}_n corresponds to the kernel of the obvious projection $\varprojlim M/M_n \rightarrow M/M_n$. In particular, the filtration topology on \hat{M} coincides with the Tychonoff product topology on $\varprojlim M/M_n$ as a subspace of $\prod M/M_n$ if each factor M/M_n is given the discrete topology. Therefore the obvious identity

$$\varprojlim \hat{M}/\hat{M}_n = \varprojlim M/M_n,$$

exactly says $\hat{M} = \hat{M}$ topologically, hence \hat{M} is complete.

We can combine filtrations and completions of rings with those of modules, as we did in the graded case. Suppose ring A is given the I -adic filtration I^n , and

suppose A module M is given an I -filtration M_n . For example, there is always the filtration $M_n = I^n M$. Now we have two completions \hat{A} and \hat{M} . But also the products $I^d \times M_n \rightarrow M_{d+n}$ induce products

$$I^d/I^{d+1} \times M_n/M_{n+1} \rightarrow M_{d+n}/M_{d+n+1} \quad \text{and} \quad \hat{A} \times \hat{M} \rightarrow \hat{M}.$$

PROPOSITION 7: The products above give \hat{M} the structure of complete topological module over the complete topological ring \hat{A} . Any two I -stable filtrations of M induce the same topology on M and hence have identical completions \hat{M} .

PROOF: Details are pretty routine and will be skipped, much as we barely gave the steps in the discussion surrounding Proposition 6. The last statement about two I -stable filtrations defining the same topology on M was already mentioned when I -stable filtrations were first introduced. Obviously, the Cauchy sequence completion of M depends only on the topology. But one can also see pretty quickly why the inverse limit completions associated to two I -stable filtrations are isomorphic.

One important example of I -adic completion is $A = \mathbb{Z}$, $I = (p)$, where p is a prime. One obtains the p -adic integers $\hat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^n \mathbb{Z}$, which can be regarded either as equivalence classes of Cauchy sequences of integers in the p -adic topology, or via the inverse limit as coherent tuples of residue classes modulo higher and higher powers of p . In this case, $\hat{\mathbb{Z}}_p$ is a compact topological ring, since the inverse limit of any system of finite sets is always compact by the Tychonoff theorem.

Another example is the polynomial ring $A = k[x_1, \dots, x_n]$, $I = (x_1, \dots, x_n)$. It is easy to see from the inverse limit construction that the completion $\hat{A} = k[[x_1, \dots, x_n]]$ is the formal power series ring.

The inverse limit construction has some delicate exactness properties. In extreme generality, an inverse limit can be defined as an object in \mathcal{D} representing a certain functor $\varprojlim F : \mathcal{D} \rightarrow \text{Sets}$ associated to a covariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$, where \mathcal{C} is a small category. Namely

$$\varprojlim F(D) \subset \prod_{C \in \mathcal{C}} \text{Hom}_{\mathcal{D}}(D, F(C))$$

is defined as the set of “coherent collections of morphisms” arising from functor F applied to all morphisms in \mathcal{C} . In our very simple case, \mathcal{C} has as objects the non-negative integers, with one morphism $m \rightarrow n$ for all $m \geq n$. So functor F is just a system of morphisms $\delta_n : D_n \rightarrow D_{n-1}$, $n \geq 1$, in \mathcal{D} .

If \mathcal{D} is the category of modules over a ring, and if $\{D_n, \delta_n\}$ is a simple inverse system with $D_0 = (0)$, define

$$d_D = \prod (\delta_n - Id_{n-1}) : \prod D_n \rightarrow \prod D_n.$$

We view d_D as the only differential in a very short chain complex. Note $\ker(d_D) = \varprojlim D_n$, the coherent tuples in $\prod D_n$. Define $\varprojlim^1 D_n = \text{coker}(d_D)$.

PROPOSITION 8: Suppose $\{A_n, \alpha_n\}, \{B_n, \beta_n\}, \{C_n, \gamma_n\}$ are three simple inverse systems of modules as above and suppose $0 \rightarrow A_n \rightarrow B_n \rightarrow C_n \rightarrow 0$ are

exact sequences commuting with the morphisms $\alpha_n, \beta_n, \gamma_n$, $n \geq 1$. Then there is a natural six term exact sequence

$$0 \rightarrow \varprojlim A_n \rightarrow \varprojlim B_n \rightarrow \varprojlim C_n \rightarrow \varprojlim^1 A_n \rightarrow \varprojlim^1 B_n \rightarrow \varprojlim^1 C_n \rightarrow 0.$$

If each morphism $\alpha_n : A_n \rightarrow A_{n-1}$ is surjective, then $\varprojlim^1 A_n = (0)$, hence

$$0 \rightarrow \varprojlim A_n \rightarrow \varprojlim B_n \rightarrow \varprojlim C_n \rightarrow 0$$

is exact.

PROOF: The six term sequence is just the ‘long’ homology exact sequence associated to the obvious short exact sequence of chain complexes with the single differentials d_A, d_B, d_C . The only homology groups are just the *kernels* and *cokernels* of these differentials.

For the second statement, note that $d_A(x_1, x_2, x_3, \dots) = (a_1, a_2, \dots) \in \prod A_n$ just says $a_1 = x_1 - \alpha_2 x_2, a_2 = x_2 - \alpha_3 x_3, \dots$. So if the α_n are surjective, we get surjectivity of d_A by choosing any x_1 , then iteratively finding suitable x_2, x_3, \dots .

The Artin-Rees theorem provides a very useful example of the results in Proposition 8. Suppose A is Noetherian and M is a finite A module with an I -stable filtration M_n , for example $M_n = I^n M$. But recall from Proposition 7, the completion $\hat{M} = \varprojlim M_n$ does not depend on the choice of I -stable filtration. Suppose $M' \subset M$ is a submodule. Then $M'_n = M' \cap M_n$ is an I -stable filtration of M' , by Artin-Rees. If we set $M'' = M/M'$ then $M''_n = \text{image}(M_n)$ is an I -stable filtration and we have exact sequences

$$0 \rightarrow M'/M'_n \rightarrow M/M_n \rightarrow M''/M''_n \rightarrow 0$$

that commute with the *surjections* in the three inverse systems.

COROLLARY 9: If A is Noetherian, M a finite A module, $M' \subset M$ a submodule, and $M'' = M/M'$ then there is a natural exact sequence of I -adic completions

$$0 \rightarrow \hat{M}' \rightarrow \hat{M} \rightarrow \hat{M}'' \rightarrow 0.$$

Thus, I -adic completion is an exact functor on the category of finite modules over a Noetherian ring.

The subtlety here is that completions can be computed from any I -stable filtrations. If we begin with $M_n = I^n M$ then it is non-trivial that $M' \cap I^n M$ is an I -stable filtration of M' . But it is exactly this filtration, rather than $I^n M'$, that fits into the exact sequence of inverse systems above.

PROPOSITION 10: If A is Noetherian, $I \subset A$ an ideal, and M a finite A module then $\hat{A} \otimes_A M \simeq \hat{M}$. Thus, \hat{A} is a flat A module.

PROOF: Begin with exact $A^p \rightarrow A^q \rightarrow M \rightarrow 0$. Then there is a diagram:

$$\begin{array}{ccccccc} \hat{A} \otimes_A A^p & \rightarrow & \hat{A} \otimes_A A^q & \rightarrow & \hat{A} \otimes_A M & \rightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \hat{A}^p & \rightarrow & \hat{A}^q & \rightarrow & \hat{M} & \rightarrow & 0 \end{array}$$

that clearly commutes. The left and center vertical arrows are isomorphisms because completion obviously commutes with finite direct sums. The top row is exact because $\hat{A} \otimes_A$ is a right exact functor. The bottom row is exact by Corollary 9, completion is exact for finite A modules. Therefore the right vertical arrow is an isomorphism.

The last statement, that \hat{A} is a flat A module, follows from the fact that one only needs to verify injectivity of $\hat{A} \otimes_A M' \rightarrow \hat{A} \otimes_A M$ when $M' \subset M$ and M' and M are finitely generated. But this follows from the first statement, because completion is exact for finite modules over Noetherian A .

We can use the results above to prove that I -adic completions of Noetherian rings are rather simple quotients of power series rings.

PROPOSITION 11: Suppose A is Noetherian, $I = (a_1, a_2, \dots, a_r) \subset A$ an ideal. Then

$$\hat{A} \simeq \frac{A[[x_1, \dots, x_r]]}{(x_j - a_j)}$$

PROOF: Set $B = A[x_1, \dots, x_r]$, $J = (x_1, \dots, x_r) \subset B$. There is an exact sequence of B modules

$$0 \rightarrow K \rightarrow B \rightarrow A \rightarrow 0$$

with $x_j \mapsto a_j$ and $K = (x_j - a_j) \subset B$. We complete in J -adic topologies, yielding exact

$$0 \rightarrow \hat{K} \rightarrow \hat{B} \rightarrow \hat{A} \rightarrow 0.$$

Note $J^n A = I^n A$, so \hat{A} is unambiguous here. Also, $\hat{B} = A[[x_1, \dots, x_r]]$ from an earlier example. Finally, $\hat{K} = K \otimes_B \hat{B} \rightarrow \hat{B}$ has image exactly $K\hat{B} = (x_j - a_j) \subset \hat{B}$. Therefore, the exact sequence of completions gives the proposition.

Next, we discuss completions of certain integral extensions of rings. Suppose A is a local Noetherian ring, with maximal ideal $m \subset A$. Suppose $A \subset B$ is an integral extension, with B finitely generated over A . Then B is a Noetherian *semilocal* ring, with maximal ideals $m_j \subset B$, $1 \leq j \leq r$, where $\sqrt{mB} = \bigcap_j m_j = \prod_j m_j = J$, the Jacobson radical of B .

In general, given ideals I, J in a ring with $J^k \subset I \subset J$ for some k , it is clear that I -adic and J -adic completions coincide. One can see this either topologically or via the inverse limit construction of completions. (Although the powers of J form an I -filtration, they form something weaker here than an I -stable filtration. Still, the topologies defined by powers of I and powers of J coincide.) We apply this to the situation above with $I = mB$, and form m -adic completions of A modules $A \subset B$.

PROPOSITION 12: If A is a local Noetherian ring with maximal ideal m and if B is a finite integral extension of A with Jacobson radical $J = \prod m_j$, then there is an inclusion of m -adic completions

$$\hat{A} \rightarrow \hat{B} \simeq \varprojlim B/J^n \simeq \varprojlim \prod_j B/m_j^n \simeq \prod_j \hat{B}_j,$$

where \hat{B}_j is the completion of B at the maximal ideal m_j .

PROOF: All that needs to be added is that we use the Chinese Remainder Theorem in the next to last isomorphism, and an obvious commutativity of operations of inverse limit and finite products in the last isomorphism.

REMARK: The m -adic completion of a local ring A at its maximal ideal is also a local ring, with isomorphic residue field $\hat{A}/\hat{m} \simeq A/m$. This is clear because an element $\vec{a} = (a_1, a_2, \dots) \in \hat{A} - \hat{m}$ if and only if $a_1 \notin m$, or equivalently $a_j \notin m$, all j . Hence \hat{a} has inverse $\hat{a}^{-1} = (a_1^{-1}, a_2^{-1}, \dots) \in \hat{A}$. So Proposition 12 embeds \hat{A} into a product of complete local rings. At each finite level, application of the Chinese Remainder Theorem $A/m^n \subset \prod_j B/m_j^{n_j}$ loses information about A .

The last result we prove is the famous lemma of Hensel.

THEOREM (Hensel): Suppose (A, m) is a *complete* local ring in the m -adic topology. (For example, the m -adic completion of any local ring.) Suppose $F(x) \in A[x]$ is a monic polynomial, with monic reduction $f(x) \in k[x]$, where $k = A/m$ is the residue field of A . Suppose $f(x) = g(x)h(x) \in k[x]$ for *relatively prime* monic polynomials g, h . Then there exist monic polynomials $G(x), H(x) \in A[x]$ such that $F(x) = G(x)H(x)$ and such that G and H reduce mod m to g and h respectively. In particular, $\deg(G) = \deg(g)$ and $\deg(H) = \deg(h)$.

REMARK: It follows that if $f(x)$ has a simple root $\alpha \in k$ then $F(x)$ has a simple root $a \in A$. Namely, a simple root is the same as a monic linear factor that does not divide the other factor.

PROOF: The idea is to inductively get $F \equiv G_n H_n \pmod{m^n[x]}$, with monic G_n, H_n reducing to g, h . The $n = 1$ case is just the hypothesis $f = gh$. Write $F(x) - G_n(x)H_n(x) = \sum y_i Q_i(x)$, with $y_i \in m^n$ and $\deg(Q_i) < \deg(F)$. Since g, h are relatively prime, we can write the mod m reduction of Q_i as $q_i = gr_i + hs_i \in k[x]$, with $\deg(r_i) < \deg(h)$. It follows that $\deg(hs_i) < \deg(F)$, hence also $\deg(s_i) < \deg(g)$.

Now lift $r_i, s_i \in k[x]$ to $R_i, S_i \in A[x]$, of the same degrees. Set

$$\begin{aligned} G_{n+1} &= G_n + \sum y_i S_i \equiv G_n \pmod{m^n[x]} \\ H_{n+1} &= H_n + \sum y_i R_i \equiv H_n \pmod{m^n[x]}. \end{aligned}$$

We then have

$$G_{n+1}H_{n+1} = G_nH_n + \sum y_i(G_nR_i + H_nS_i).$$

But

$$G_nR_i + H_nS_i \equiv Q_i \pmod{m[x]}.$$

Therefore

$$F \equiv G_{n+1}H_{n+1} \pmod{m^{n+1}[x]}.$$

We now obtain the theorem by taking $G = \lim(G_n)$ and $H = \lim(H_n)$ in the complete local ring A .