Chapter 4

Completion

The set $\mathbb{R}$ of real numbers is a complete metric space in which the set $\mathbb{Q}$ of rationals is dense. In fact any metric space can be embedded as a dense subset of a complete metric space. The construction is a familiar one involving equivalence classes of Cauchy sequences. We will see that under appropriate conditions, this procedure can be generalized to modules.

4.1 Graded Rings and Modules

4.1.1 Definitions and Comments

A *graded ring* is a ring R that is expressible as $\oplus_{n\geq 0}R_n$ where the R_n are additive subgroups such that $R_mR_n \subseteq R_{m+n}$. Sometimes, R_n is referred to as the n^{th} *graded piece* and elements of R_n are said to be *homogeneous of degree* n. The prototype is a polynomial ring in several variables, with R_d consisting of all homogeneous polynomials of degree d (along with the zero polynomial). A *graded module* over a graded ring R is a module M expressible as $\oplus_{n\geq 0}M_n$, where $R_mM_n \subseteq M_{m+n}$.

Note that the identity element of a graded ring R must belong to R_0. For if 1 has a component a of maximum degree $n > 0$, then $1a = a$ forces the degree of a to exceed n, a contradiction.

Now suppose that $\{R_n\}$ is a *filtration* of the ring R, in other words, the R_n are additive subgroups such that

$$R = R_0 \supseteq R_1 \supseteq \cdots \supseteq R_n \supseteq \cdots$$

with $R_mR_n \subseteq R_{m+n}$. We call R a *filtered ring*. A *filtered module*

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq \cdots$$

over the filtered ring R may be defined similarly. In this case, each M_n is a submodule and we require that $R_mM_n \subseteq M_{m+n}$.

If I is an ideal of the ring R and M is an R-module, we will be interested in the *I-adic filtrations* of R and of M, given respectively by $R_n = I^n$ and $M_n = I^nM$. (Take $I^0 = R$, so that $M_0 = M$.)

4.1.2 Associated Graded Rings and Modules

If $\{R_n\}$ is a filtration of R, the *associated graded ring* of R is defined as

$$\mathrm{gr}(R) = \bigoplus_{n\geq 0} \mathrm{gr}_n(R)$$

where $\mathrm{gr}_n(R) = R_n/R_{n+1}$. We must be careful in defining multiplication in $\mathrm{gr}(R)$. If $a \in R_m$ and $b \in R_n$, then $a + R_{m+1} \in R_m/R_{m+1}$ and $b + R_{n+1} \in R_n/R_{n+1}$. We take

$$(a + R_{m+1})(b + R_{n+1}) = ab + R_{m+n+1}$$

so that the product of an element of $\mathrm{gr}_m(R)$ and an element of $\mathrm{gr}_n(R)$ will belong to $\mathrm{gr}_{m+n}(R)$. If $a \in R_{m+1}$ and $b \in R_n$, then $ab \in R_{m+n+1}$, so multiplication is well-defined.

If M is a filtered module over a filtered ring R, we define the *associated graded module* of M as

$$\mathrm{gr}(M) = \bigoplus_{n\geq 0} \mathrm{gr}_n(M)$$

where $\mathrm{gr}_n(M) = M_n/M_{n+1}$. If $a \in R_m$ and $x \in M_n$, we define scalar multiplication by

$$(a + R_{m+1})(x + M_{n+1}) = ax + M_{m+n+1}$$

and it follows that

$$(R_m/R_{m+1})(M_n/M_{n+1}) \subseteq M_{m+n}/M_{m+n+1}.$$

Thus $\mathrm{gr}(M)$ is a graded module over the graded ring $\mathrm{gr}(R)$.

It is natural to ask for conditions under which a graded ring will be Noetherian, and the behavior of the subring R_0 is critical.

4.1.3 Proposition

Let $R = \oplus_{d\geq 0} R_d$ be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is a finitely generated R_0-algebra.

Proof. If the condition on R_0 holds, then R is a quotient of a polynomial ring $R_0[X_1, \ldots, X_n]$, hence R is Noetherian by the Hilbert Basis Theorem. Conversely, if R is Noetherian, then so is R_0, because $R_0 \cong R/I$ where I is the ideal $\oplus_{d\geq 1} R_d$. By hypothesis, I is finitely generated, say by homogeneous elements $a_1, \ldots, a_r$ of degree $n_1, \ldots, n_r$ respectively. Let $R' = R_0[a_1, \ldots, a_r]$ be the R_0-subalgebra of R generated by the a_i. It suffices to show that $R_n \subseteq R'$ for all $n \geq 0$ (and therefore $R = R'$). We have $R_0 \subseteq R'$ by definition of R', so assume as an induction hypothesis that $R_d \subseteq R'$ for $d \leq n-1$, where $n > 0$. If $a \in R_n$, then a can be expressed as $c_1 a_1 + \cdots + c_r a_r$, where c_i $(i = 1, \ldots, r)$ must be a homogeneous element of degree $n - n_i < n = \deg a$. By induction hypothesis, $c_i \in R'$, and since $a_i \in R'$ we have $a \in R'$. ♣

We now prepare for the basic Artin-Rees lemma.

4.1.4 Definitions and Comments

Let M be a filtered R-module with filtration $\{M_n\}$, I an ideal of R. We say that $\{M_n\}$ is an *I-filtration* if $IM_n \subseteq M_{n+1}$ for all n. An I-filtration with $IM_n = M_{n+1}$ for all sufficiently large n is said to be *I-stable*. Note that the I-adic filtration is I-stable.

4.1.5 Proposition

Let M be a finitely generated module over a Noetherian ring R, and suppose that $\{M_n\}$ is an I-filtration of M. The following conditions are equivalent.

1. $\{M_n\}$ is I-stable.
2. Define a graded ring R^* and a graded R^*-module M^* by

$$R^* = \bigoplus_{n\geq 0} I^n, \quad M^* = \bigoplus_{n\geq 0} M_n.$$

Then M^* is finitely generated.

Proof. Let $N_n = \oplus_{i=0}^n M_i$, and define

$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2M_n \oplus \cdots$$

Since N_n is finitely generated over R, it follows that M_n^* is a finitely generated R^*-module. By definition, M^* is the union of the M_n^* over all $n \geq 0$. Therefore M^* is finitely generated over R^* if and only if $M^* = M_m^*$ for some m, in other words, $M_{m+k} = I^k M_m$ for all $k \geq 1$. Equivalently, the filtration $\{M_n\}$ is I-stable. ♣

4.1.6 Induced Filtrations

If $\{M_n\}$ is a filtration of the R-module M, and N is a submodule of M, then we have filtrations induced on N and M/N, given by $N_n = N \cap M_n$ and $(M/N)_n = (M_n + N)/N$ respectively.

4.1.7 Artin-Rees Lemma

Let M be a finitely generated module over the Noetherian ring R, and assume that M has an I-stable filtration $\{M_n\}$, where I is an ideal of R. Let N be a submodule of M. Then the filtration $\{N_n = N \cap M_n\}$ induced by M on N is also I-stable.

Proof. As in (4.1.5), let $R^* = \oplus_{n\geq 0} I^n$, $M^* = \oplus_{n\geq 0} M_n$, and $N^* = \oplus_{n\geq 0} N_n$. Since R is Noetherian, I is finitely generated, so R^* is a finitely generated R-algebra. (Elements of R^* can be expressed as polynomials in a finite set of generators of I.) By (4.1.3), R^* is a Noetherian ring. Now by hypothesis, M is finitely generated over the Noetherian ring R and $\{M_n\}$ is I-stable, so by (4.1.5), M^* is finitely generated over R^*. Therefore the submodule N^* is also finitely generated over R^*. Again using (4.1.5), we conclude that $\{N_n\}$ is I-stable. ♣

4.1.8 Applications

Let M be a finitely generated module over the Noetherian ring R, with N a submodule of M. The filtration on N induced by the I-adic filtration on M is given by $N_m = (I^m M) \cap N$. By Artin-Rees, for large enough m we have

$$I^k((I^m M) \cap N) = (I^{m+k} M) \cap N$$

for all $k \geq 0$.

There is a basic topological interpretation of this result. We can make M into a topological abelian group in which the module operations are continuous. The sets $I^m M$ are a base for the neighborhoods of 0, and the translations $x + I^m M$ form a basis for the neighborhoods of an arbitrary point $x \in M$. The resulting topology is called the *I-adic topology* on M. The above equation says that the I-adic topology on N coincides with the topology induced on N by the I-adic topology on M.

4.2 Completion of a Module

4.2.1 Inverse Limits

Suppose we have countably many R-modules $M_0, M_1, \ldots,$ with R-module homomorphisms $\theta_n : M_n \to M_{n-1}, n \geq 1$. (We are restricting to the countable case to simplify the notation, but the ideas carry over to an arbitrary family of modules, indexed by a directed set. If $i \leq j$, we have a homomorphism f_{ij} from M_j to M_i. We assume that the maps can be composed consistently, in other words, if $i \leq j \leq k$, then $f_{ij} \circ f_{jk} = f_{ik}$.)The collection of modules and maps is called an *inverse system*.

A sequence (x_i) in the direct product $\prod M_i$ is said to be *coherent* if it respects the maps θ_n in the sense that for every i we have $\theta_{i+1}(x_{i+1}) = x_i$. The collection M of all coherent sequences is called the *inverse limit* of the inverse system. The inverse limit is denoted by

$$\varprojlim M_n.$$

Note that M becomes an R-module with componentwise addition and scalar multiplication of coherent sequences, in other words, $(x_i) + (y_i) = (x_i + y_i)$ and $r(x_i) = (rx_i)$.

Now suppose that we have homomorphisms g_i from an R-module M' to $M_i, i = 0, 1, \ldots$. Call the g_i *coherent* if $\theta_{i+1} \circ g_{i+1} = g_i$ for all i. Then the g_i can be lifted to a homomorphism g from M' to M. Explicitly, $g(x) = (g_i(x))$, and the coherence of the g_i forces the sequence $(g_i(x))$ to be coherent.

An inverse limit of an inverse system of rings can be constructed in a similar fashion, as coherent sequences can be multiplied componentwise, that is, $(x_i)(y_i) = (x_i y_i)$.

4.2.2 Examples

1. Take $R = \mathbb{Z}$, and let I be the ideal (p) where p is a fixed prime. Take $M_n = \mathbb{Z}/I^n$ and $\theta_{n+1}(a + I^{n+1}) = a + I^n$. The inverse limit of the M_n is the ring $\mathbb{Z}_p$ of p-adic integers.

2. Let $R = A[x_1, \dots, x_n]$ be a polynomial ring in n variables, and I the maximal ideal $(x_1, \dots, x_n)$. Let $M_n = R/I^n$ and $\theta_n(f + I^n) = f + I^{n-1}, n = 1, 2, \dots$. An element of M_n is represented by a polynomial f of degree at most $n-1$. (We take the degree of f to be the maximum degree of a monomial in f.) The image of f in I^{n-1} is represented by the same polynomial with the terms of degree $n-1$ deleted. Thus the inverse limit can be identified with the ring $A[[x_1, \dots, x_n]]$ of formal power series.

Now let M be a filtered R-module with filtration $\{M_n\}$. The filtration determines a topology on M as in (4.1.8), with the M_n forming a base for the neighborhoods of 0. We have the following result.

4.2.3 Proposition

If N is a submodule of M, then the closure of N is given by $\overline{N} = \cap_{n=0}^{\infty}(N + M_n)$.

Proof. Let x be an element of M. Then x fails to belong to $\overline{N}$ iff some neighborhood of x is disjoint from N, in other words, $(x+M_n)\cap N = \emptyset$ for some n. Equivalently, $x \notin N+M_n$ for some n, and the result follows. To justify the last step, note that if $x \in N + M_n$, then $x = y + z,\ y \in N,\ z \in M_n$. Thus $y = x - z \in (x + M_n) \cap N$. Conversely, if $y \in (x + M_n) \cap N$, then for some $z \in M_n$ we have $y = x - z$, so $x = y + z \in N + M_n$. ♣

4.2.4 Corollary

The topology is Hausdorff if and only if $\cap_{n=0}^{\infty} M_n = \{0\}$.

Proof. By (4.2.3), $\cap_{n=0}^{\infty} M_n = \overline{\{0\}}$, so we are asserting that the Hausdorff property is equivalent to points being closed, that is, the T_1 condition. This holds because separating distinct points x and y by disjoint open sets is equivalent to separating $x - y$ from 0. ♣

4.2.5 Definition of the Completion

Let $\{M_n\}$ be a filtration of the R-module M. Recalling the construction of the reals from the rationals, or the process of completing an arbitrary metric space, let us try to come up with something similar in this case. If we go far out in a Cauchy sequence, the difference between terms becomes small. Thus we can define a *Cauchy sequence* $\{x_n\}$ *in* M by the requirement that for every positive integer r there is a positive integer N such that $x_n - x_m \in M_r$ for $n, m \geq N$. We identify the Cauchy sequences $\{x_n\}$ and $\{y_n\}$ if they get close to each other for large n. More precisely, given a positive integer r there exists a positive integer N such that $x_n - y_n \in M_r$ for all $n \geq N$. Notice that the condition $x_n - x_m \in M_r$ is equivalent to $x_n + M_r = x_m + M_r$. This suggests that the essential feature of the Cauchy condition is that the sequence is coherent with respect to the maps $\theta_n : M/M_n \to M/M_{n-1}$. Motivated by this observation, we define the *completion* of M as

$$\hat{M} = \varprojlim (M/M_n).$$

The functor that assigns the inverse limit to an inverse system of modules is left exact, and becomes exact under certain conditions.

4.2.6 Theorem

Let $\{M'_n, \theta'_n\}$, $\{M_n, \theta_n\}$, and $\{M''_n, \theta''_n\}$ be inverse systems of modules, and assume that the diagram below is commutative with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'_{n+1} & \xrightarrow{f_{n+1}} & M_{n+1} & \xrightarrow{g_{n+1}} & M''_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta'_{n+1}} & & \downarrow{\scriptstyle \theta_{n+1}} & & \downarrow{\scriptstyle \theta''_{n+1}} & & \\ 0 & \longrightarrow & M'_n & \xrightarrow{f_n} & M_n & \xrightarrow{g_n} & M''_n & \longrightarrow & 0 \end{array}$$

Then the sequence

$$0 \to \varprojlim M'_n \to \varprojlim M_n \to \varprojlim M''_n$$

is exact. If θ'_n is surjective for all n, then

$$0 \to \varprojlim M'_n \to \varprojlim M_n \to \varprojlim M''_n \to 0$$

is exact.

Proof. Let $M = \prod M_n$ and define an R- homomorphism $d_M : M \to M$ by $d_M(x_n) = (x_n - \theta_{n+1}(x_{n+1}))$. The kernel of d_M is the inverse limit of the M_n. Now the maps (f_n) and (g_n) induce $f = \prod f_n : M' = \prod M'_n \to M$ and $g = \prod g_n : M \to M'' = \prod M''_n$. We have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_{M'}} & & \downarrow{\scriptstyle d_M} & & \downarrow{\scriptstyle d_{M''}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \end{array}$$

We now apply the snake lemma, which is discussed in detail in TBGY (Section S2 of the supplement). The result is an exact sequence

$$0 \to \ker d_{M'} \to \ker d_M \to \ker d_{M''} \to \operatorname{coker}\ d_{M'},$$

proving the first assertion. If θ'_n is surjective for all n, then $d_{M'}$ is surjective, and consequently the cokernel of $d_{M'}$ is 0. The second assertion follows. ♣

4.2.7 Corollary

Suppose that the sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact. Let $\{M_n\}$ be a filtration of M, so that $\{M_n\}$ induces filtrations $\{M' \cap f^{-1}(M_n)\}$ and $\{g(M_n)\}$ on M' and M'' respectively. Then the sequence

$$0 \to (M')\hat{} \to \hat{M} \to (M'')\hat{} \to 0$$

is exact.

Proof. Exactness of the given sequence implies that the diagram below is commutative with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'/(M' \cap f^{-1}(M_{n+1})) & \longrightarrow & M/M_{n+1} & \longrightarrow & M''/g(M_{n+1}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta'_{n+1}} & & \downarrow{\scriptstyle \theta_{n+1}} & & \downarrow{\scriptstyle \theta''_{n+1}} & & \\ 0 & \longrightarrow & M'/(M' \cap f^{-1}(M_n)) & \longrightarrow & M/M_n & \longrightarrow & M''/g(M_n) & \longrightarrow & 0 \end{array}$$

Since θ'_n is surjective for all n, (4.2.6) allows us to pass to the inverse limit. ♣

4.2.8 Remark

A filtration $\{M_n\}$ of an R-module M induces in a natural way a filtration $\{N \cap M_n\}$ on a given submodule N, and a filtration $\{(N + M_n)/N\}$ on the quotient module M/N. We have already noted this in (4.2.7) (with f the inclusion map and g the canonical epimorphism), but the point is worth emphasizing.

4.2.9 Corollary

Let $\{M_n\}$ be a filtration of the R-module M. Let $\hat{M}_n$ be the completion of M_n with respect to the induced filtration on M_n [see (4.2.8)]. Then $\hat{M}_n$ is a submodule of $\hat{M}$ and $\hat{M}/\hat{M}_n \cong M/M_n$ for all n.

Proof. We apply (4.2.7) with $M' = M_n$ and $M'' = M/M_n$, to obtain the exact sequence

$$0 \to \hat{M}_n \to \hat{M} \to (M/M_n)\hat{} \to 0.$$

Thus we may identify $\hat{M}_n$ with a submodule of $\hat{M}$, and

$$\hat{M}/\hat{M}_n \cong (M/M_n)\hat{} = (M'')\hat{}.$$

Now the m^{th} term of the induced filtration on M'' is

$$M''_m = (M_n + M_m)/M_n = M_n/M_n = 0$$

for $m \geq n$. Thus M'' has the discrete topology, so Cauchy sequences (and coherent sequences) can be identified with single points. Therefore M'' is isomorphic to its completion, and we have $\hat{M}/\hat{M}_n \cong M/M_n$ for every n. ♣

4.2.10 Remarks

Two filtrations $\{M_n\}$ and $\{M'_n\}$ of a given R-module are said to be *equivalent* if they induce the same topology. For example, under the hypothesis of (4.1.8), the filtrations $\{I^n N\}$ and $\{N \cap I^n M\}$ of the submodule N are equivalent (Problem 5). Since equivalent filtrations give rise to the same set of Cauchy sequences, it follows that completions of a given module with respect to equivalent filtrations are isomorphic.

4.3 The Krull Intersection Theorem

4.3.1 Definitions and Comments

Recall from (4.1.1) and (4.1.8) that the I-adic topology on the R-module M is the topology induced on M by the I-adic filtration $M_n = I^n M$. The completion of M with respect to the I-adic filtration is called the *I-adic completion*.

There is a natural map from a filtered module M to its completion $\hat{M}$ given by $x \to \{x + M_n\}$. The kernel of this map is $\cap_{n=0}^{\infty} M_n$, which is $\cap_{n=0}^{\infty} I^n M$ if the filtration is I-adic. The Krull intersection theorem (4.3.2) gives precise information about this kernel.

4.3.2 Theorem

Let M be a finitely generated module over the Noetherian ring R, I an ideal of R, and $\hat{M}$ the I-adic completion of M. Let N be the kernel of the natural map $M \to \hat{M}$. Then N is the set of elements $x \in M$ such that x is annihilated by some element of $1 + I$. In fact, we can find a single element of $1 + I$ that works for the entire kernel.

Proof. Suppose that $a \in I$, $x \in M$, and $(1 + a)x = 0$. Then

$$x = -ax = -a(-ax) = a^2x = a^2(-ax) = -a^3x = a^4x = \cdots,$$

hence $x \in I^n M$ for all $n \geq 0$. Conversely, we must show that for some $a \in I$, $1 + a$ annihilates everything in the kernel N. By (4.1.8), for some n we have, for all $k \geq 0$,

$$I^k((I^n M) \cap N) = (I^{n+k} M) \cap N.$$

Set $k = 1$ to get

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

But $N \subseteq I^{n+1} M \subseteq I^n M$, so the above equation says that $IN = N$. By (0.3.1), there exists $a \in I$ such that $(1 + a)N = 0$. ♣

4.3.3 Corollary

If I is a proper ideal of the Noetherian integral domain R, then $\cap_{n=0}^{\infty} I^n = 0$.

Proof. The intersection of the I^n is the kernel N of the natural map from R to $\hat{R}$. By (4.3.2), $1 + a$ annihilates N for some $a \in I$. If $0 \neq x \in N$ then $(1 + a)x = 0$, and since R is a domain, $1 + a = 0$. But then -1, hence 1, belongs to I, contradicting the hypothesis that I is proper. ♣

4.3.4 Corollary

Let M be a finitely generated module over the Noetherian ring R. If the ideal I of R is contained in the Jacobson radical $J(R)$, then $\cap_{n=0}^{\infty} I^n M = 0$. Thus by (4.2.4), the I-adic topology on M is Hausdorff.

Proof. Let $a \in I \subseteq J(R)$ be such that $(1 + a)$ annihilates the kernel $N = \cap_{n=0}^{\infty} I^n M$ of the natural map from M to $\hat{M}$. By (0.2.1), $1 + a$ is a unit of R, so if $x \in N$ (hence $(1 + a)x = 0$), we have $x = 0$. ♣

4.3.5 Corollary

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$. If M is a finitely generated R-module, then $\cap_{n=0}^{\infty}\mathcal{M}^n M = 0$. Thus the $\mathcal{M}$-adic topology on M, in particular the $\mathcal{M}$-adic topology on R, is Hausdorff.

Proof. Since $\mathcal{M} = J(R)$, this follows from (4.3.4). ♣

4.4 Hensel's Lemma

Let A be a local ring with maximal ideal P, and let $k = A/P$ be the residue field. Assume that A is complete with respect to the P-adic topology, in other words, every Cauchy sequence converges. In algebraic number theory, where this result is most often applied, A is a discrete valuation ring of a local field. But the statement and proof of the algebraic number theory result can be copied, as follows.

If $a \in A$, then the coset $a + P \in k$ will be denoted by $\overline{a}$. If f is a polynomial in $A[X]$, then reduction of the coefficients of f mod P yields a polynomial $\overline{f}$ in $k[X]$. Thus

$$f(X) = \sum_{i=0}^{d} a_i X^i \in A[X],\ \overline{f}(X) = \sum_{i=0}^{d} \overline{a}_i X^i \in k[X].$$

Hensel's lemma is about lifting a factorization of $\overline{f}$ from $k[X]$ to $A[X]$. Here is the precise statement.

4.4.1 Hensel's Lemma

Assume that f is a monic polynomial of degree d in $A[X]$, and that the corresponding polynomial $F = \overline{f}$ factors as the product of relatively prime monic polynomials G and H in $k[X]$. Then there are monic polynomials g and h in $A[X]$ such that $\overline{g} = G,\ \overline{h} = H$ and $f = gh$.

Proof. Let r be the degree of G, so that $\deg H = d - r$. We will inductively construct $g_n, h_n \in A[X], n = 1, 2, \ldots$, such that $\deg g_n = r,\ \deg h_n = d - r,\ \overline{g}_n = G,\ \overline{h}_n = H$, and

$$f(X) - g_n(X)h_n(X) \in P^n[X].$$

Thus the coefficients of $f - g_n h_n$ belong to P^n.

The basis step: Let $n = 1$. Choose monic $g_1, h_1 \in A[X]$ such that $\overline{g}_1 = G$ and $\overline{h}_1 = H$. Then $\deg g_1 = r$ and $\deg h_1 = d - r$. Since $\overline{f} = \overline{g}_1\overline{h}_1$, we have $f - g_1 h_1 \in P[X]$.

The inductive step: Assume that g_n and h_n have been constructed. Let $f(X) - g_n(X)h_n(X) = \sum_{i=0}^{d} c_i X^i$ with the $c_i \in P^n$. Since $G = \overline{g}_n$ and $H = \overline{h}_n$ are relatively prime, for each $i = 0, \ldots, d$ there are polynomials $\overline{v}_i$ and $\overline{w}_i$ in $k[X]$ such that

$$X^i = \overline{v}_i(X)\overline{g}_n(X) + \overline{w}_i(X)\overline{h}_n(X).$$

Since $\overline{g}_n$ has degree r, the degree of $\overline{v}_i$ is at most $d - r$, and similarly the degree of $\overline{w}_i$ is at most r. Moreover,

$$X^i - v_i(X)g_n(X) - w_i(X)h_n(X) \in P[X]. \qquad (1)$$

We define

$$g_{n+1}(X) = g_n(X) + \sum_{i=0}^{d} c_i w_i(X),\ h_{n+1}(X) = h_n(X) + \sum_{i=0}^{d} c_i v_i(X).$$

Since the c_i belong to $P^n \subseteq P$, it follows that $\overline{g}_{n+1} = \overline{g}_n = G$ and $\overline{h}_{n+1} = \overline{h}_n = H$. Since the degree of g_{n+1} is at most r, it must be exactly r, and similarly the degree of h_{n+1} is $d - r$. To check the remaining condition,

$$f - g_{n+1}h_{n+1} = f - (g_n + \sum_i c_i w_i)(h_n + \sum_i c_i v_i)$$

$$= (f - g_n h_n - \sum_i c_i X^i) + \sum_i c_i (X^i - g_n v_i - h_n w_i) - \sum_{i,j} c_i c_j w_i v_j.$$

By the induction hypothesis, the first grouped term on the right is zero, and, with the aid of Equation (1) above, the second grouped term belongs to $P^n P[X] = P^{n+1}[X]$. The final term belongs to $P^{2n}[X] \subseteq P^{n+1}[X]$, completing the induction.

Finishing the proof. By definition of g_{n+1}, we have $g_{n+1} - g_n \in P^n[X]$, so for any fixed i, the sequence of coefficients of X^i in $g_n(X)$ is Cauchy and therefore converges. To simplify the notation we write $g_n(X) \to g(X)$, and similarly $h_n(X) \to h(X)$, with $g(X), h(X) \in A[X]$. By construction, $f - g_n h_n \in P^n[X]$, and we may let $n \to \infty$ to get $f = gh$. Since $\overline{g}_n = G$ and $\overline{h}_n = H$ for all n, we must have $\overline{g} = G$ and $\overline{h} = H$. Since f, G and H are monic, the highest degree terms of g and h are of the form $(1 + a)X^r$ and $(1 + a)^{-1}X^{d-r}$ respectively, with $a \in P$. (Note that $1 + a$ must reduce to 1 mod P.) By replacing g and h by $(1 + a)^{-1}g$ and $(1 + a)h$, respectively, we can make g and h monic without disturbing the other conditions. The proof is complete. ♣