Formal power series rings, inverse limits, and I-adic completions of rings

Formal semigroup rings and formal power series rings

We next want to explore the notion of a (formal) power series ring in finitely many variables over a ring R, and show that it is Noetherian when R is. But we begin with a definition in much greater generality.

Let S be a commutative semigroup (which will have identity $1_S = 1$) written multiplicatively. The *semigroup ring* of S with coefficients in R may be thought of as the free R-module with basis S, with multiplication defined by the rule

$$(\sum_{i=1}^{h} r_i s_i)(\sum_{j=1}^{k} r'_j s'_j) = \sum_{s \in S}(\sum_{s_i s'_j = s} r_i r'_j)s.$$

We next want to construct a much larger ring in which infinite sums of multiples of elements of S are allowed. In order to insure that multiplication is well-defined, from now on we assume that S has the following additional property:

(#) For all $s \in S$, $\{(s_1, s_2) \in S \times S : s_1 s_2 = s\}$ is finite.

Thus, each element of S has only finitely many factorizations as a product of two elements. For example, we may take S to be the set of all monomials $\{x_1^{k_1} \cdots x_n^{k_n} : (k_1, \ldots, k_n) \in \mathbb{N}^n\}$ in n variables. For this chocie of S, the usual semigroup ring $R[S]$ may be identified with the polynomial ring $R[x_1, \ldots, x_n]$ in n indeterminates over R.

We next construct a *formal semigroup* ring denoted $R[[S]]$: we may think of this ring formally as consisting of all functions from S to R, but we shall indicate elements of the ring notationally as (possibly infinite) formal sums $\sum_{s \in S} r_s s$, where the function corresponding to this formal sum maps s to r_s for all $s \in S$. Addition is performed by adding corresponding coefficients, while $(\sum_{s \in S} r_s s)(\sum_{s' \in S} r_{s'} s')$ is defined to be

$$\sum_{t \in S}(\sum_{s, s' \in S, ss' = t} r_s r_{s'})t.$$

Heuristically, this is what one would get by distributing the product in all possible ways, and then "collecting terms": this is possible because, by (#), only finitely many terms $r_s r_{s'} ss'$ occur for any particular $t = ss'$. The ring has identity corresponding to the sum in which 1_S has coefficient $1 = 1_R$ and all other coefficients are 0. It is straightforward to verify all the ring laws and the commutativity of multiplication. $R[S]$, the semigroup ring defined earlier, is a subring: it may be identified with the formal sums in which all but finitely many coefficients are 0. One frequently omits terms with coefficient 0 from the notation. If $S = \{x_1^{k_1} \cdots x_n^{k_n} : (k_1, \ldots, k_n) \in \mathbb{N}^N\}$, the notation $R[[x_1, \ldots, x_n]]$ is used instead of $R[[S]]$: one writes generators for S inside the double brackets instead of S itself.

If S and S' both satisfy (#), so does the product semigroup $S \times S'$, and one has the isomorphism $(R[[S]])[[S']] \cong R[[S \times S']]$. If the coefficient of s' in an element of the former is $\sum_{s \in S} r_{s,s'} s$ for every $s' \in S'$, one identifies $\sum_{s' \in S'} (\sum_{s \in S} r_{s,s'} s) s'$ with $\sum_{(s,s') \in S \times S'} r_{s,s'} (ss')$. It is straightforward to check that this is an isomorphism.

The ring $R[[x_1, \ldots, x_n]]$ is referred to as a *(formal) power series* ring over R, and the x_i are called *formal* or *analytic* indeterminates to indicate that two power series agree if and only if their corresponding coefficients are all identical.

In the case of two finitely generated semigroups of monomials, the fact that $R[[S \times S']] \cong (R[[S]])[[S']]$ implies that

$$(R[[x_1, \ldots, x_n]])[[y_1, \ldots, y_m]] \cong R[[x_1, \ldots, x_n, y_1, \ldots, y_m]].$$

In particular, for $n \geq 2$,

$$R[[x_1, \ldots, x_n]] \cong (R[[x_1, \ldots, x_{n-1}]])[[x_n]].$$

Of course, there is a completely analogous statement for polynomial rings, with single brackets replacing double brackets. However, note that while

$$(R[[x_1, \ldots, x_n]])[y_1, \ldots, y_m] \hookrightarrow (R[y_1, \ldots, y_m])[[x_1, \ldots, x_n]],$$

the opposite inclusion always fails when R is not 0 and $m, n \geq 1$. First, to see the inclusion, note that if one has a homomorphism $h : R \to T$ there is an induced homomorphism $R[[x_1, \ldots, x_n]] \to T[[x_1, \ldots, x_n]]$: apply h to every coefficient. Let $T = R[y_1, \ldots, y_m]$ and h be the inclusion $R \subseteq T$ to get an injection

$$R[[x_1, \ldots, x_n]] \to (R[y_1, \ldots, y_m])[[x_1, \ldots, x_n]].$$

Now extend this homomorphism of $R[[x_1, \ldots, x_n]]$-algebras to the polynomial ring

$$(R[[x_1, \ldots, x_n]])[y_1, \ldots, y_m]$$

by letting y_i map to $y_i \in (R[y_1, \ldots, y_m])[[x_1, \ldots, x_n]]$. To see that the inclusion is typically strict, note that $\sum_{t=0}^{\infty} y_1^t x_1^t$ is an element of $(R[y_1, \ldots, y_m])[[x_1, \ldots, x_n]]$ but is not in $(R[[x_1, \ldots, x_n]])[y_1, \ldots, y_m]$, where every element has bounded degree in the y_j. Both rings inject into $R[[x_1, \ldots, x_n, y_1, \ldots, y_m]]$.

Theorem. *If R is Noetherian ring then the formal power series ring $R[[x_1, \ldots, x_n]]$ is Noetherian.*

Proof. By induction on the number of variables one reduces at once to proving that $S = R[[x]]$ is Noetherian. Let $J \subseteq R[[x]]$ be an ideal. Let I_t denote the set of elements r of R such that rx^n is the term of least degree in an element of J, together with 0. This is easily verified to be an ideal of R. If $f \in J$ is not zero, and rx^n is the least degree term in f, then rx^{n+1} is the least degree term in $xf \in J$. This shows that $\{I_t\}_{t \geq 0}$ is a non-decreasing sequence of ideals of R. Since R is Noetherian, we may choose $k \in \mathbb{N}$

such that $I_k = I_{k+1} = \cdots = I_{k+m} = \cdots$, and then for $0 \le t \le k$ we may choose $f_{1,t}, \ldots, f_{h_t,t} \in J$ such that each $f_{i,t}$ has smallest degree term of the form $r_{i,t}x^t$ and the elements $r_{i,t}, \ldots, r_{h_t,t}$ are a finite set of generators of I_t. We claim that the finite set of power series $f_{i,t}$, $0 \le t \le k$, $1 \le i \le h_t$, generates J. Let J_0 be the ideal they generate, and let $u \in J$ be given. We may subtract an R-linear combination of the $f_{i,0}$ from u to get an element of J whose lowest degree term is in degree at least one (or such that the difference is 0). We continue in this way so long as we have a lowest degree term of degree less than k: if the degree is $t < k$, we may increase it by subtracting an R-linear combination of the $f_{i,t}$. Thus, after subtracting an element of J_0 from u, we may assume without loss of generality that the lowest degree term in u occurs in degree $\ge k$ (or else u is 0, but then there is nothing to prove). It will suffice to prove that this new choice of u is in J_0. We claim more: we shall show that in this case, u is in the ideal generated by the $f_{i,k} = f_i$. Let $h = h_k$. We recursively construct the partial sums (which are polynomials) of power series g_i such that $u = \sum_{i=1}^h g_i f_i$.

Put slightly differently and more precisely, we shall construct, for every i, $1 \le i \le h$, by induction on $m \in \mathbb{N}$, a sequence of polynomials $g_{i,m}(x) \in R[x]$ with the following properties:

(1) Every $g_{i,m}$ has degree at most m.
(2) If $m_1 < m_2$ then g_{i,m_1} is the sum of the terms of degree at most m_1 that occur in g_{i,m_2}. Given (1), this is equivalent to the condition that for all $m \ge 0$, $g_{i,m+1} - g_{i,m}$ has the form rx^{m+1} for some $r \in R$, which may be 0.
(3) For every m, the lowest degree term in $u - \sum_{i=1}^h g_{i,m} f_i$ has degree at least $k + m + 1$ (or else the difference is 0).

Notice that conditions (1) and (2) together imply that for every i, the $g_{i,m}$ are the partial sums of a formal power series, where the m th partial sum of a power series $\sum_{j=0}^\infty r_j x^j$ is defined to be $\sum_{j=0}^m r_j x^j$.

To begin the induction, note that the least degree term of u occurs in degree k or higher. Therefore the coefficient of x^k in u is in the ideal generated by the lowest degree coefficients of $f_1, \ldots, f_h$, and it follows that there are elements $r_{1,0}, \ldots, r_{h,0}$ of R such that the lowest degree term of $u - \sum_{i=1}^h r_{i,0} f_i$ occurs in degree at least $k + 1$ (or the difference is 0). We take $g_{i,0} = r_{i,0}$, $1 \le i \le h$.

Now suppose that the $g_{i,s}$ have been constructed for $1 \le i \le h$, $0 \le s \le m$ such that conditions (1), (2), and (3) are satisfied. We shall show that we can construct $g_{i,m+1}$ so that (1), (2), and (3) are satisfied. Since $u' = u - \sum_{i=1}^h g_{i,m} f_i$ has lowest degree term of degree at least $m + k + 1$, the coefficient of x^{m+k+1} is in the R-span of the coefficients of x^k in the polynomials f_i, and so we can choose elements $r_{i,m+1} \in R$ so that $u' - \sum_{i=1}^h r_{i,m+1} x^{m+1} f_i$ has lowest degree term in degree at least $m + k + 2$ (or is 0). It follows that if we take $g_{i,m+1} = g_{i,m} + r_{i,m+1} x^{m+1}$ for $1 \le i \le h$, then (1) and (2) are satisfied, and (3) is as well because $u - \sum_{i=1}^h g_{i,m+1} f_i = u' - \sum_{i=1}^h r_{i,m+1} x^{m+1} f_i$ has lowest degree term in degree at least $m + k + 2$ (or the difference is 0). For each i, $1 \le i \le h$, let g_i be the formal power series whose partial sums are the $g_{i,m}$.

We claim that $u = \sum_{i=1}^h g_i f_i$. It suffices to show that the coefficients on corresponding powers of x are the same on both sides. Neither side has a nonzero term involving x^t for $t < k$. On the other hand, for all $m \geq 0$, the coefficient of x^{k+m} on the right will not change if we replace every g_i on the right by $g_{i,m}$, since $g_i - g_{i,m}$ involves only terms of degree strictly bigger than $m + k + 1$. Thus, it suffices to show that for all $m \geq 0$, the difference $u - \sum_{i=1}^h g_{i,m} f_i$ has coefficient 0 on x^{m+k}, and this is true by part (3). But the $f_i = f_{i,k}$ are in J_0, so that $u \in J_0$, as required. $\square$

It is also true that the subring of $\mathbb{C}[[x_1, \ldots, x_n]]$ (respectively, $\mathbb{R}[[x_1, \ldots, x_n]]$) consisting of power series that converge on a neighborhood of the origin in $\mathbb{C}^n$ (respectively, $\mathbb{R}^n$) is a Noetherian ring with a unique maximal ideal, generated by $x_1, \ldots, x_n$. These rings are denoted $\mathbb{C}\langle\langle x_1, \ldots, x_n\rangle\rangle$ and $\mathbb{R}\langle\langle x_1, \ldots, x_n\rangle\rangle$, respectively.

The Noetherian property of the ring $\mathbb{C}\langle\langle x_1, \ldots, x_n\rangle\rangle$ is of considerable usefulness in studying functions of several complex variables: this is the ring of germs of holomorphic functions at a point in $\mathbb{C}^n$. We shall not give the proof of the Noetherian property for convergent power series rings here: proofs may be found in [O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Van Nostrand, Princeton, 1960], pp. 142–148 or [M. Nagata, *Local Rings*, Interscience, New York, 1962], pp. 190–194.

Inverse limits

Let $(\Lambda, \leq)$ be a directed set. By an *inverse limit system* in a category $\mathcal{C}$ indexed by Λ we mean a family of objects X_λ indexed by Λ and for all $\lambda \leq \mu$ a morphism $f_{\lambda,\mu} : X_\mu \to X_\lambda$. A candidate for the inverse limit consists of an object X together with maps $g_\lambda : X \to X_\lambda$ such that for all $\lambda \leq \mu$, $g_\lambda = f_{\lambda,\mu} \circ g_\mu$. A candidate Y together with morphisms $h_\lambda : Y \to X_\lambda$ is an inverse limit precisely if for every candidate (X, g_λ) there is a unique morphism $k : X \to Y$ such that for all λ, $g_\lambda = h_\lambda \circ k$. The inverse limit is denoted $\varprojlim_\lambda X_\lambda$ and, if it exists, it is unique up to canonical isomorphism compatible with the morphisms giving X and Y the structure of candidates.

We next want to see that inverse limits exist in the categories of sets, abelian groups, rings, R-modules, and R-algebras. The construction for sets also works in the other categories mentioned. Let $(\Lambda, \leq)$ be a directed partially ordered set and let $(X_\lambda, f_{\lambda,\mu})$ be an inverse limit system of sets. Consider the subset $X \subseteq \prod_\lambda X_\lambda$ consisting of all elements x of the product such that for $\lambda \leq \mu$, $f_{\lambda,\mu}(x_\mu) = x_\lambda$, where x_λ and x_μ are the λ and μ coordinates, respectively, of x. It is straightforward to verify that X is an inverse limit for the system: the maps $X \to X_\lambda$ are obtained by composing the inclusion of X in the product with the product projections π_λ mapping the product to X_λ.

If each X_λ is in one of the categories specified above, notice that the Cartesian product is as well, and the set X is easily verified to be a subobject in the appropriate category. In every instance, it is straightforward to check that X is an inverse limit.

Suppose, for example, that X_λ is a family of subsets of A ordered by $\supseteq$, and that the map $X_\mu \to X_\lambda$ for $X_\lambda \supseteq X_\mu$ is the inclusion of $X_\mu \subseteq X_\lambda$. The condition for the partially ordered set to be directed is that for all λ and μ, there is a set in the family contained in

$X_\lambda \cap X_\mu$. The construction for the inverse limit given above yields all functions on these sets with a constant value in the intersection of all of them. This set evidently may be identified with $\bigcap_\lambda X_\lambda$.

We are particularly interested in inverse limit systems indexed by $\mathbb{N}$. To give such a system one needs to give an infinite sequence of objects $X_0,\ X_1,\ X_2,\ \ldots$ in the category and for every $i \geq 0$ a map $X_{i+1} \to X_i$. The other maps needed can be obtained from these by composition. In the cases of the categories mentioned above, to give an element of the inverse limit is the same a giving a sequence of elements $x_0,\ x_1,\ x_2,\ \ldots$ such that for all i, $x_i \in X_i$, and x_{i+1} maps to x_i for all $i \geq 0$. One can attempt to construct an element of the inverse limit by choosing an element $x_0 \in X_0$, then choosing an element $x_1 \in X_1$ that maps to x_0, etc. If the maps are all surjective, then given $x_i \in X_i$ one can always find an element of the inverse limit that has x_i as its ith coordinate: for $h < i$, use the image of x_i in X_h, while for $i+1, i+2, \ldots$ one can choose values recursively, using the surjectivity of the maps.

The *I*-adic competion of a ring

We want to use these ideas to describe the I-adic completion of a ring R, where R is a ring and $I \subseteq R$ is an ideal. We give two alternative descriptions. Consider the set of all sequences of elements of R indexed by $\mathbb{N}$ under termwise addition under multiplication: this ring is the same as the product of a family of copies of R index by $\mathbb{N}$. Let $\mathfrak{C}_I(R)$ denote the subring of *Cauchy sequences for the I-adic topology*: by definition these are the sequences such that for all $t \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that for all $i,\ j \geq N$, $r_i - r_j \in I^t$. This is a subring of the ring of sequences. It is an R-algebra via the map $R \to \mathfrak{C}_I(R)$ that sends $r \in R$ to the constant sequence $r,\ r,\ r,\ \ldots$. Let $\mathfrak{C}_i^0(R)$ be the set of *Cauchy sequences that converge to 0*: by definition, these are the sequences such that for all $t \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that for all $i \geq N$, $r_i \in I^t$. These sequences are automatically Cauchy. Then $\mathfrak{C}_I^0(R)$ is an ideal of $\mathfrak{C}_I(R)$. It is easy to verify that every subsequence of a Cauchy sequence is again Cauchy, and that it differs from the original sequence by an element of $\mathfrak{C}_I^0(R)$.

Given an element of $\mathfrak{C}_I(R)$, say $r_0, r_1, r_2, \ldots$ we may consider the residue mod I^t for a given t. These are eventually all the same, by the definition of a Cauchy sequence. The stable value of these residues is an element of R/I^t, and we thus have a map $\mathfrak{C}_I(R) \twoheadrightarrow R/I^t$ that is easily seen to be a ring homomorphism that kills $\mathfrak{C}_I^0(R)$. Therefore, for all t we have a surjection $\mathfrak{C}_I(R)/\mathfrak{C}_I^0(R) \twoheadrightarrow R/I^t$. These maps make $\mathfrak{C}_I(R)/\mathfrak{C}_I^0(R)$ a candidate for $\varprojlim_t (R/I^t)$, and so induce a ring homomorphism $\mathfrak{C}_I(R)/\mathfrak{C}_i^0(R) \to \varprojlim_t R/I^t$.

This map is an isomorphism. Given a sequence of elements in the rings R/I^t that determine an element of the inverse limit, for each residue ρ_t choose an element r_t of R that represents it. It is straightforward to verify that the r_t form a Cauchy sequence in R and that it maps to the element of $\varprojlim_t R/I^t$ with which we started. Consider any other Cauchy sequence with the same image. It is again straightforward to verify that the difference of the two Cauchy sequences is in $\mathfrak{C}_i^0(R)$. This proves the isomorphism:

Theorem. *Let R be any ring and I any ideal. Then $\mathfrak{C}_I(R)/\mathfrak{C}^0_I(R) \to \varprojlim_t (R/I^t)$ is an isomorphism, and the kernel of the map from R to either of these isomorphic R-algebras is $\cap_t I^t$.* $\square$

These isomorphic rings are denoted $\widehat{R}^I$ or simply $\widehat{R}$, if I is understood, and either is referred to as the *I-adic completion* of R. If $I \subseteq R$, then R is called I-adically separated if $\bigcap_t I^t = (0)$, and I-adically complete if $R \to \widehat{R}^I$ is an isomorphism: this holds iff R is I-adically separated, and every Cauchy sequence is the sum of a constant sequence $r, r, r, \ldots$ and a sequence that converges to 0. The Cauchy sequence is said to *converge* to r.

Given a Cauchy sequence in R with respect to I, we may choose a subsequence such that the residues of all terms from the t th on are constant mod I^{t+1}. Call such a Cauchy sequence *standard*. Given a standard Cauchy sequence, let $s_0 = r_0$ and $s_{t+1} = r_{t+1} - r_t \in I^t$ for $t \geq 0$. Then the $s_0 + \cdots + s_t = r_t$. Thus, the partial sums of the "formal series" $s_0 + s_1 + s_2 + \cdots$ form a Cauchy sequence, and if the ring is complete it converges. Given any formal series $\sum_{t=0}^{\infty} s_t$ such that $s_t \in I^t$ for all t, the partial sums form a Cauchy sequence, and every Cauchy sequence is obtained, up to equivalence (i.e., up to adding a sequence that converges to 0) in this way.

Proposition. *Let J denote the kernel of the map from $\widehat{R}^I \twoheadrightarrow R/I$ (J consists of elements represented by Cauchy sequences all of whose terms are in I). Then every element of $\widehat{R}^I$ that is the sum of a unit and an element of J is invertible in $\widehat{R}^I$. Every maximal ideal of $\widehat{R}^I$ contains J, and so there is a bijection between the maximal ideals of $\widehat{R}^I$ and the maximal ideals of R/I. In particular, if R/I is quasi-local, then $\widehat{R}^I$ is quasi-local.*

Proof. If u is a unit and $j \in J$ we may write $u = u(1 + u^{-1}j)$, and so it suffices to to show that $1 + j$ is invertible for $j \in J$. Let $r_0, r_1, \ldots$ be a Cauchy sequence that represents j. Consider the sequence $1 - r_0, 1 - r_1 + r_1^2, \ldots 1 - r_n + r_n^2 - \cdots + (-1)^{n-1} r_n^{n+1}, \cdots$: call the n th term of this sequence v_n. If r_n and r_{n+1} differ by an element of I^t, then v_n and v_{n+1} differ by an element of $I^t + I^{n+2}$. ¿From this it follows that v_n is a Cauchy sequence, and $1 - (1 + r_n)v_n = r_n^{n+2}$ converges to 0. Thus, the sequence v_n represents an inverse for $1 + j$ in $\widehat{R}^I$.

Suppose that m is a maximal ideal of $\widehat{R}^I$ and does not contain $j \in J$. Then j has an inverse v mod m, so that we have $jv = 1 + u$ where $u \in m$, and then $-u = 1 - jv$ is not invertible, a contradiction, since $jv \in J$. $\square$

Suppose that $\bigcap_t I^t = 0$. We define the distance $d(r, s)$ between two elements $r, s \in R$ to be 0 if $r = s$, and otherwise to be $1/2^n$ (this choice is somewhat arbitrary), where n is the largest integer such that $r - s \in I^n$. This is a metric on R: given three elements $r, s, t \in R$, the triangle inequality is clearly satisfied if any two of them are equal. If not, let n, p, q be the largest powers of I containing $r - s$, $s - t$, and $t - r$, respectively. Since $t - r = -(s - t) - (r - s)$, $q \geq \min\{n, p\}$, with equality unless $n = p$. It follows that in every "triangle," the two largest sides (or all three sides) are equal, which implies the triangle inequality. The notion of Cauchy sequence that we have given is the same as the notion of Cauchy sequence for this metric. Thus, $\widehat{R}^I$ is literally the completion of R as a metric space with respect to this metric.

Given a ring homomorphism $R \to R'$ mapping I into an ideal I' of R', Cauchy sequences in R with respect to I map to Cauchy sequences in R' with respect to I', and Cauchy sequences that converge to 0 map to Cauchy sequences that converge to 0. Thus, we get an induced ring homomorphism $\widehat{R}^I \to \widehat{R'}^{I'}$. This construction is functorial in the sense that if we have a map to a third ring R'', a ring homomorphism $R' \to R''$, and an ideal I'' of R'' such that I' maps into I'', then the induced map $\widehat{R}^I \to \widehat{R''}^{I''}$ is the composition $(\widehat{R'}^{I'} \to \widehat{R''}^{I''}) \circ (\widehat{R}^I \to \widehat{R'}^{I'})$. If $R \to R'$ is surjective and I maps onto I', then the map of completions is surjective: each element of $\widehat{R'}^{I'}$ can be represented as the partial sums of a series $s_0 + s_1 + s_2 + \cdots$, where $s_n \in (I')^n$. But I^n will map onto $(I')^n$, and so we can find $r_n \in I^n$ that maps to s_n, and then $r_0 + r_1 + r_2 \cdots$ represents an element of $\widehat{R}^I$ that maps to $s_0 + s_1 + s_2 + \cdots$.

Example. Let $S = R[x_1, \ldots, x_n]$ be the polynomial ring in n variables over R, and let $I = (x_1, \ldots, x_n)S$. An element of S/I^n is represented by a polynomial of degree $\leq n-1$ in the x_i. A sequence of such polynomials will represent an element of the inverse limit if and only if, for every n, then n th term is precisely the sum of the terms of degree at most n in the $n+1$ st term. It follows that the inverse limit ring $\widehat{S}^I$ is $R[[x_1, \ldots, x_n]]$, the formal power series ring. In consequence, we can prove:

Theorem. *If R is a Noetherian ring and I is an ideal of R, then $\widehat{R}^I$ is Noetherian.*

Proof. Suppose that $I = (f_1, \ldots, f_n)R$. Map the polynomial ring $S = R[x_1, \ldots, x_n]$ to R as an R-algebra by letting $x_j \mapsto f_j$. This is surjective, and $(x_1, \ldots, x_n)S$ maps onto I. Therefore we get a surjection $R[[x_1, \ldots, x_n]] \twoheadrightarrow \widehat{R}^I$. Since we already know that the formal power series ring is Noetherian, it follows that $\widehat{R}^I$ is Noetherian. $\square$

We next want to form the I-adic completion of an R-module M. This will be not only an R-module: it will also be a module over $\widehat{R}^I$. Let R be a ring, $I \subseteq R$ an ideal and M an R-module. Let $\mathfrak{C}_I(M)$ denote the Cauchy sequences in M with respect to I: the sequence $u_0, u_1, u_2, \cdots$ is a *Cauchy sequence* if for all $t \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that $u_i - u_j \in I^t M$ for all $i, j \geq N$. These form a module over $\mathfrak{C}_I(R)$ under termwise multiplication, and set of Cauchy sequences, $\mathfrak{C}_I^0(M)$, that converge to 0, where this means that for all t, the terms of the sequence are eventually all in $I^t M$, is a submodule that contains $\mathfrak{C}_I^0(R)\mathfrak{C}_I(M)$. The quotient $\mathfrak{C}_I(M)/\mathfrak{C}_I^0(M)$ is consequently a module over $\widehat{R}^I$. Moreover, any homomorphism $h : M \to N$ induces a homomorphism from $\mathfrak{C}_I(M) \to \mathfrak{C}_I(N)$ that preserves convergence to 0, and hence a homomorphism $\widehat{h}^I : \widehat{M}^I \to \widehat{N}^I$. This is a covariant functor from R-modules to $\widehat{R}^I$-modules. There is an R-linear map $M \to \widehat{M}^I$ that sends the element u to the element represented by the constant Cauchy sequence whose terms are all u. The kernel of this map is $\bigcap_t I^t M$, and so it is injective if and only if $\bigcap_t I^t M = 0$, in which case M is called *I-adically separated.* If $M \to \widehat{M}^I$ is an isomorphism, M is called *I-adically complete*. The maps $M \to \widehat{M}^I$ give a natural transformation from the identity functor on R-modules to the I-adic completion functor. Moreover, by exactly the same reasoning as in the case where $M = R$, $\widehat{M}^I \cong \varprojlim_t M/I^t M$.

I-adic completion commutes in an obvious way with finite direct sums and products (which may be identified in the category of R-modules). The point is that $u_n \oplus v_n$ gives a Cauchy sequence (respectively, a sequence converging to 0) in $M \oplus N$ if and only if u_n and v_n give such sequences in M and N. Moreover if $f_1 : M_1 \to N$ and $f_2 : M_2 \to N$, we have that the I-adic completion of the map $f_1 \oplus f_2 : M_1 \oplus M_2 \to N$ is the direct sum of the completions, $\widehat{f_1} \oplus \widehat{f_2}$. A similar remark applies when we have $g_1 : M \to N_1$ and $g_2 : M \to N_2$, and we consider the map $(g_1, g_2) : M \to N_1 \times N_2$. The situation is the same for finite direct sums and finite direct products. Note also that if we consider the map given by multiplication by r on M, the induced endomorphism of $\widehat{M}^I$ is given by multiplication by r (or by the image of r in $\widehat{R}^I$).

If $M \to Q$ is surjective, the map $\widehat{M}^I \to \widehat{Q}^I$ is surjective: as in the case of rings, any element z of $\widehat{Q}^I$ can be represented using the Cauchy sequence of partial sums of a formal series $q_0 + q_1 + q_2 + \cdots$ where $q_t \in I^t Q$. To see this, take a Cauchy sequence that represents the element. Pass to a subsequence $w_0, w_1, w_2, \ldots$ such that the residue of w_k in M/I^tM is the same for all $k \geq t$. The element can be thought of as

$$w_0 + (w_1 - w_0) + (w_2 - w_1) + \cdots .$$

Thus, take $q_0 = w_0$ and $q_t = w_t - w_{t-1}$ for $t \geq 1$. For all t, I^tM maps onto I^tQ. Therefore we can find $u_t \in I^tM$ such that u_t maps to q_t, and the partial sums of $u_0 + u_1 + u_2 + \cdots$ represent an element of $\widehat{M}^I$ that maps to z.

Note that because $\widehat{M}^I$ is an R-module and we have a canonical map $M \to \widehat{M}^I$ that is R-linear, the universal property of base change determines a map $\widehat{R}^I \otimes_R M \to \widehat{M}^I$. These maps give a natural transformation from the functor $\widehat{R}^I \otimes_R \_$ to the I-adic completion functor: these are both functors from R-modules to $\widehat{R}^I$-modules. If M is finitely generated over a Noetherian ring R, this map is an isomorphism: not only that: restricted to finitely generated modules, I-adic completion is an exact functor, and $\widehat{R}^I$ is flat over R.

In order to prove this, we need to prove the famous Artin-Rees Lemma. Let R be a ring and I an ideal of R. Let t be an indeterminate, and let $It = \{it : i \in I\} \subseteq R[t]$. Then $R[It] = R + It + I^2t^2 + \cdots$ is called the *Rees ring* of I. If $I = (f_1, \ldots, f_n)$ is finitely generated as an ideal, then $R[It] = R[f_1t, \ldots, f_nt]$ is a finitely generated R-algebra. Therefore, the Rees ring is Noetherian if R is.

Before proving the Artin-Rees theorem, we note that if M is an R-module and t and indeterminate, then every element of $R[t] \otimes M$ can be written uniquely in the form

$$1 \otimes u_0 + t \otimes u_1 + \cdots + t^k \otimes u_k,$$

where the $u_j \in M$, for any sufficiently large k: if a larger integer s is used, then one has $m_{k+1} = \cdots = m_s = 0$. This is a consequence of the fact that $R[t]$ is R-free with the powers of t as a free basis. Frequently one writes $u_0 + u_1t + \cdots + u_kt^k$ instead, which looks like a polynomial in t with coefficients in M. When this notation is used, $M[t]$ is used as a notation for the module. Note that the $R[t]$-module structure is suggested by the notation: $(rt^j)(ut^k) = (ru)t^{j+k}$, and all other more general instances of multiplication are then determined by the distributive law.

We are now ready to prove the Artin-Rees Theorem, which is due independently to Emil Artin and David Rees.

Theorem (E. Artin, D. Rees). *Let $N \subseteq M$ be Noetherian modules over the Noetherian ring R and let I be an ideal of R. Then there is a constant positive integer c such that for all $n \geq c$, $I^nM \cap N = I^{n-c}(I^cM \cap N)$. That is, eventually, each of the modules $N_{n+1} = I^{n+1}M \cap N$ is I times its predecessor, $N_n = I^nM \cap N$.*

In particular, there is a constant c such that $I^nM \cap N \subseteq I^{n-c}N$ for all $n \geq c$. In consequence, if a sequence of elements in N is an I-adic Cauchy sequence in M (respectively, converges to 0 in M) then it is an I-adic Cauchy sequence in N (respectively, converges to 0 in N).

Proof. We consider the module $R[t] \otimes M$, which we think of as $M[t]$. Within this module,

$$\mathcal{M} = M + IMt + I^2Mt^2 + \cdots + I^kMt^k + \cdots$$

is a finitely generated $R[It]$-module, generated by generators for M as an R-module: this is straightforward. Therefore, $\mathcal{M}$ is Noetherian over $R[It]$. But

$$\mathcal{N} = N + (IM \cap N)t + (I^2M \cap N)t^2 + \cdots ,$$

which may also be described as $N[t] \cap \mathcal{M}$, is an $R[It]$ submodule of $\mathcal{M}$, and so finitely generated over $R[It]$. Therefore for some $c \in \mathbb{N}$ we can choose a finite set of generators whose degrees in t are all at most c. By breaking the generators into summands homogeneous with respect to t, we see that we may use elements from

$$N, (IM \cap N)t, (I^2M \cap N)t^2, \ldots , (I^cM \cap N)t^c$$

as generators. Now suppose that $n \geq c$ and that $u \in I^nM \cap N$. Then ut^n can be written as an $R[It]$-linear combination of of elements from

$$N, (IM \cap N)t, (I^2M \cap N)t^2, \ldots , (I^cM \cap N)t^c,$$

and hence as an sum of terms of the form

$$i_h t^h v_j t^j = (i_h v_j)t^{h+j}$$

where $j \leq c$, $i_h \in I^h$, and

$$v_j \in I^jM \cap N.$$

Of course, one only needs to use those terms such that $h + j = n$. This shows that $(I^nM) \cap N$ is the sum of the modules

$$I^{n-j}(I^jM \cap N)$$

for $j \leq c$. But

$$I^{n-j}(I^jM \cap N) = I^{n-c}I^{c-j}(I^jM \cap N),$$

and

$$I^{c-j}(I^jM \cap N) \subseteq I^cM \cap N,$$

so that we only need the single term $I^{n-c}(I^cM \cap N)$. $\square$

Theorem. *Let R be a Noetherian ring, $I \subseteq R$ an ideal.*
(a) *If $0 \to N \to M \to Q \to 0$ is a short exact sequence of finitely generated R-modules, then the sequence $0 \to \widehat{N}^I \to \widehat{M}^I \to \widehat{Q}^I \to 0$ is exact. That is, I-adic completion is an exact functor on finitely generated R-modules.*
(b) *The natural transformation θ from $\widehat{R}^I \otimes_R \_$ to the I-adic completion functor is an isomorphism of functors on finitely generated R-modules. That is, for every finitely generated R-module M, the natural map $\theta_M : \widehat{R}^I \otimes_R M \to \widehat{M}^I$ is an isomorphism.*
(c) *$\widehat{R}^I$ is a flat R-algebra. If (R, m) is local, $\widehat{R} = \widehat{R}^m$ is a faithfully flat local R-algebra.*

Proof. (a) We have already seen that the map $\widehat{M}^I \to \widehat{Q}^I$ is surjective. Let y be an element of $\widehat{M}^I$ that maps to 0 in $\widehat{Q}$. Choose a Cauchy sequence that represents z, say $u_0, u_1, u_2, \ldots$. After passing to a subsequence we may assume that $u_t - u_{t+1} \in I^tM$ for every t. The images of the u_t in $Q \cong M/N$ converge to 0. Passing to a further subsequence we may assume that the image of $u_t \in I^t(M/N)$ for all t, so that $u^t \in I^tM + N$, say $u_t = v_t + w_t$ where $v_t \in I^tM$ and $w_t \in N$. Then w_t is a Cauchy sequence in M that represents z: in fact, $w_t - w_{t+1} \in I^tM \cap N$ for all t. Each $w_t \in N$, and so the elements w_t form a Cauchy sequence in N, by the Artin-Rees Theorem. Thus, every element in $\mathrm{Ker}\,(\widehat{M}^I \to \widehat{Q}^I)$ is in the image of $\widehat{N}^I$.

Finally, suppose that $z_0, z_1, z_2, \ldots$ is a Cauchy sequence in N that converges to 0 in M. Then z_t already converges to 0 in N, and this shows that $\widehat{N}^I$ injects into $\widehat{M}^I$. This completes the proof of part (a).

(b) Take a presentation of M, say $R^n \xrightarrow{A} R^m \to M \to 0$, where $A = (r_{ij})$ is an $m \times n$ matrix over R. This yields a diagram:

$$\begin{tikzcd}
\widehat{R}^I \otimes_R R^n \arrow[r, "A"] & \widehat{R}^I \otimes_R R^m \arrow[r] & \widehat{R}^I \otimes_R M \arrow[r] & 0 \\
\widehat{R^n}^I \arrow[u, "\theta_{R^n}"] \arrow[r, "A"] & \widehat{R^m}^I \arrow[u, "\theta_{R^m}"] \arrow[r] & \widehat{M}^I \arrow[u, "\theta_M"] \arrow[r] & 0
\end{tikzcd}$$

where the top row is obtained by applying $\widehat{R}^I \otimes \_$, and is exact by the right exactness of tensor, the bottom row is obtained by applying the I-adic completion functor, and is exact by part (a). The vertical arrows are given by the natural transformation θ, and the squares commute because θ is natural. The map θ_{R^h} is an isomorphism for $h = m$ or $h = n$ because both functors commute with direct sum, and the case where the free module is just R is obvious. But then θ_M is an isomorphism, because cokernels of isomorphic maps are isomorphic.

(c) We must show that $\widehat{R}^I \otimes_R N \to \widehat{R}^I \otimes_R M$ is injective for every pair of R-modules $N \subseteq M$. We know this from parts (a) and (b) when the modules are finitely generated. The result now follows from the Lemma just below. Faithful flatness is clear, since the maximal ideal of R clearly expands to a proper ideal in $\widehat{R}^I$. $\square$

Lemma. *Let F be an R-module, and suppose that whenever $N \subseteq M$ are finitely generated R-modules then $F \otimes_R N \to F \otimes_R M$ is injective. Then F is flat.*

Proof. Let $N \subseteq M$ be arbitrary R-modules. Then $F \otimes_R N$ is the directed union of the images of the modules $F \otimes_R N_0$ as F runs through the finitely generated submodules of M. Thus, if $z \in F \otimes N$ maps to 0 in $F \otimes M$, it will be the image of $z' \in N_0 \otimes M - \{0\}$, which implies that $z' \in F \otimes_R N_0$ maps to 0 in $F \otimes_R M$. But since M is the directed union of its finitely generated modules M_0 containing N_0, and since $F \otimes_R M$ is the direct limit of these, it follows that for some sufficiently large but finitely generated $M_0 \supseteq N_0$, the image of z' under the map $F \otimes N_0 \to F \otimes M_0$ is 0. But then $z' = 0$ and so $z = 0$, as required. $\square$