Reading Project: Rings and Modules

Shantanu Nene

May 2022

1 What properties of R also hold for $R[x]$?

1. Commutativity.
   Also holds for $R[x]$.

2. No zero divisors.
   Also holds for $R[x]$.

3. Noetherian.
   Also holds for $R[x]$. Using Hilbert's Basis Theorem. Holds for non-commutative case as well (left/right Noetherian implies left/right Noetherian respectively).

4. R is a PID.
   May not hold for $R[x]$. Counterexample: $R = \mathbb{Z}$. The ideal $\langle x, 2\rangle$ is non-principal in $\mathbb{Z}[x]$.

5. There is an $M > 0$ such that all ideals in R can be generated by at most M elements.
   May not hold for $R[x]$. Counterexample: $R = \mathbb{Q}[x]$. For any $n > 0$, look at the ideal $\langle y^n, y^{n-1}x, y^{n-2}x^2, \dots x^n\rangle$ of $\mathbb{Q}[x, y]$. Note that this is just $\langle x, y\rangle^n$. The minimal generating set of this has size $n + 1$.
   Proof: Assume that there is a smaller generating set. Therefore there are some $f_1, f_2, \dots f_n$ such that every $y^i x^{n-i}$ can be written as a linear combination of the f_j over $\mathbb{Q}[x, y]$:

   $$y^i x^{n-i} = \sum_{j=1}^{n} g_{ij}(x, y) f_j(x, y)$$

   Now, since each f_j is in $\langle x, y\rangle^n$, the degree of each monomial in f_j is at least n. Since the LHS has degree n, every higher order term in the RHS gets cancelled. Hence we can assume each g_ij is actually constant, since otherwise any non-constant terms just produce a term with order greater than n. Then, using the fact that $\mathbb{Q}[x, y]$ is a vector space over Q, some element $y^i x^{n-i}$ can be written as a linear combination of other elements, say $\sum_{j\neq i} a_j y^j x^{n-j}$ for some rationals a_j. By looking at degrees, we see that f_j for $j < i$ are 0. But then, all terms of RHS have order at least y^{i+1}, which is not true for the LHS, contradiction!

   We can instead take $\mathbb{Z}$ in the above example. The corresponding ideals are then $\langle x, 2\rangle$ and $\langle x, 2\rangle^n = \langle x^n, 2x^{n-1}, 2^2x^{n-2}, \dots 2^n\rangle$. For a proof, consider the same ideal $I = \langle x, 2\rangle^n$ in the ring $\mathbb{Z}[x]/\langle x, 2\rangle^{n+1}$. We claim that this ideal is in fact a vector space over $\mathbb{Z}/2\mathbb{Z}$. Indeed, we have $2^i x^{n-i} + 2^i x^{n-i} = 0$ for each i, so the same holds true for all elements generated by them. Further, we see that every element of I can be written as a linear combination of the $2^i x^{n-i}$ over $\mathbb{Z}/2\mathbb{Z}$, i.e., all the coefficients are 0 or 1. Now we can finish the proof in the same way as above.

6. R satisfies ACC on principal ideals.
   Also holds for $R[x]$.
   Proof: Assume $(f_1) \subset (f_2) \subset (f_3) \cdots$ is an ascending sequence of principal ideals. Then

$f_{n+1} \mid f_n$, so $\deg(f_{n+1}) \leq \deg(f_n)$. The degree cannot keep on decreasing forever, so after some point it must become constant. Suppose $f_N, f_{N+1}, \ldots$ have the same degree. Then their leading coefficients, say $a_N, a_{N+1}, \ldots$ satisfy $(a_N) \subset (a_{N+1}) \subset \cdots$, so they must become constant due to ACC on R. Thus the leading coefficients and degrees become constant, and because of the divisibility condition, f_n must become constant as well.

7. R is a UFD.
   Also holds for $R[x]$.
   Proof: By the above point, $R[x]$ also has ACC on principal ideals. This implies that every polynomial can be factored into irreducibles, otherwise we have an infinite ascending chain of principal ideals. Now we just have to prove that it is unique. Let K be the field of fractions R. Then $K[x]$ is a UFD because it is a Euclidean domain. Also by Gauss's lemma, a polynomial is irreducible in $K[x]$ iff it is irreducible in $R[x]$, and thus $R[x]$ is UFD as well.

8. R is a skew field.
   May not hold for $R[x]$. x does not have an inverse.

9. R is a Euclidean domain.
   May not hold for $R[x]$. Counterexample: $R = \mathbb{Z}$. Every Euclidean domain is a PID, but $\mathbb{Z}[x]$ is not that.

10. R has no nilpotent elements.
    Also holds for $R[x]$. This even holds in the non-commutative case.
    Proof: Suppose f is nilpotent, with leading coefficient a. Then $f^n = 0$ for some n, but its leading coefficient is $a^n \neq 0$.

2 What properties of R also hold for $R[[x]]$?

We use the following property of $R[[x]]$: a power series f is a unit iff it has order 0 and its constant term is a unit in R. This is proved in a later section.

1. Commutativity.
   Also holds for $R[[x]]$.

2. No zero divisors.
   Also holds for $R[[x]]$. We look at the coefficient of the smallest order terms.

3. Noetherian.
   Probably also holds for $R[[x]]$. Proof is done in the section "Primes in Noetherian Rings".

4. R is a PID.
   May not hold for $R[[x]]$. Again consider $R = \mathbb{Z}$. Then $\langle x, 2\rangle$ is again not principal.
   Proof: Assume some power series f divides both x and 2. Since it divides x, its constant term divides 1, so is ± 1. Therefore f is a unit, and so the ideal is the entire ring. But this is impossible because for any power series in $\langle x, 2\rangle$, its constant term must be divisible by 2.

5. There is an $M > 0$ such that all ideals in R can be generated by at most M elements.
   May not hold for $R[[x]]$. Basically the same counterexample as in the polynomial case ($R = \mathbb{Q}[x]$ and $\langle x, y\rangle^n$), and the same proof, but with power series (in y) in place of polynomials (note that $\mathbb{Q}[x][[y]]$ is also a vector space over $\mathbb{Q}$). Again $\mathbb{Z}$ works with $\langle x, 2\rangle^n$ here as well, with the same proof.

6. R satisfies ACC on principal ideals.
   Also holds for $R[x]$. Basically the same proof as in the polynomial case, but with power series replaced for polynomials, and degree replaced by order. Except at the end, we get the orders

and leading coefficients to become constant; then if $f_n = g \cdot f_{n+1}$, g must have constant term 1, so g is still units, and the ideals are the same.

7. R is a UFD.
   May not hold for $R[[x]]$. Counterexample: Take $R = k[x, y, z]/(x^2+y^3+z^7)$ localized at (x, y, z), where k is a field of characteristic 2.

8. R is a skew field.
   May not hold for $R[[x]]$. x does not have an inverse.

9. R is a Euclidean domain.
   May not hold for $R[[x]]$. Counterexample: $R = \mathbb{Z}$. Every Euclidean domain is a PID, but $\mathbb{Z}[[x]]$ is not that.

10. R has no nilpotent elements.
    Also holds for $R[[x]]$. This even holds in the non-commutative case.
    Proof: Suppose f is nilpotent, with leading coefficient a (i.e., coefficient of term with smallest order). Then $f^n = 0$ for some n, but its leading coefficient is $a^n \neq 0$.

3 Quotient Rings

We only look at commutative rings in this section.

Theorem 1. *Let R be a ring, and I be an ideal of R. Then there is a one-to-one correspondence between ideals of R/I and ideals of R containing I. The explicit correspondence is given by $J \to J/I$.*

In particular, maximal ideals of R/I correspond to maximal ideals of R containing I. Also prime ideals of R/I correspond to prime ideals of R containing I, and radical ideals of R/I correspond to radical ideals of R containing I; this is because both kinds of ideals operate on the concept of $ab \in J \implies a \in J$ or $b \in J$, which stays invariant while lifting.

Theorem 2. *Let I, J be ideals of a ring R such that $I + J = R$. Then $I \cap J = IJ$, and*

$$R/I \cap J \cong R/I \times R/J$$

Proof. We first prove that $I \cap J = IJ$. Indeed, $IJ \subset I \cap J$, so let $a \in I \cap J$ be arbitrary. Then there exist $b \in I$ and $c \in J$ such that $b + c = 1$. Therefore $a = a(b + c) = ab + ac$, but both $ab, ac \in IJ$. Thus $a \in IJ$, as required.

Now for the second part. Consider the map $\phi : R \to R/I \times R/J$ given by $a \to (a + I, a + J)$. This is clearly a homomorphism. We show that this is surjective. Indeed, for any $b, c \in R$, we can write $b = b_1 + b_2$ and $c = c_1 + c_2$ where $b_1, c_1 \in I$ and $b_2, c_2 \in J$. Then $b + I = b_2 + I = b_2 + c_1 + I$, and $c + J = c_1 + J = c_1 + b_2 + J$. Therefore $\phi(c_1 + b_2) = (b + I, c + J)$, as required. Also, the kernel of this homomorphism is the set of all a that are in both I, J, i.e., $I \cap J$. Therefore the isomorphism follows from the first isomorphism theorem. □

Definition. Two ideals $I, J \subseteq R$ are called comaximal if $I + J = R$

The above theorem can be generalized:

Theorem 3 (Chinese Remainder Theorem)**.** *Let $I_1, I_2, \ldots I_n$ be pairwise comaximal ideals. Then the intersection of all the I_j is $I_1 I_2 \cdots I_n$, and*

$$R/I_1 I_2 \cdots I_n \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

Proof. We use the first theorem and induction on n. To proceed by induction, it is enough to prove that if I, J, K are pairwise comaximal, then IJ and K are comaximal. Indeed, there exist $a \in I$, $b \in J$, and $c, d \in K$ such that $a + c = b + d = 1$. Therefore,

$$ab + bc + ad + cd = (a + c)(b + d) = 1$$

Since $ab \in IJ$ and $bc + ad + cd \in K$, we get $1 \in IJ + K \implies IJ + K = R$, as required. Now we can easily prove the theorem just by induction. If it is true for $n - 1$, then we apply the above theorem to $I_1 I_2 \cdots I_{n-1}$ and I_n. □

Theorem 4. *Let I, J be comaximal ideals of R. Then for any positive integers m, n, I^m and J^n are also comaximal.*

Proof. If $a \in I$ and $b \in J$ such that $a + b = 1$, then $(a + b)^{m+n} = 1$ as well. However, by directly expanding we can check that $(a + b)^{m+n} \in I^m + J^n$, as required. □

Local rings can be characterized using comaximal ideals as well:

Theorem 5. *A ring R is local iff it contains no pair of proper comaximal ideals.*

Proof. If a ring is local, then all proper ideals are contained in its maximal ideal, and so sum of any two of them is contained in the maximal ideal as well, so it cannot be R. Conversely, if R is not local, then there exist two distinct maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2$ in R, which must also be comaximal. □

In particular, no local ring can be decomposed as a direct sum of proper non-zero ideals. The best we can get is a decomposition of the maximal ideal. For example, the ring $k[x, y]/\langle x^2, xy, y^2\rangle$, where k is a field, is local with maximal ideal $\langle x, y\rangle$. We can write it as a direct sum $\langle x, y\rangle = \langle x\rangle \oplus \langle y\rangle$. Such local rings can be realized as a fiber product of two quotient rings. For instance, $k[x, y]/\langle x^2, xy, y^2\rangle$ is the fiber product $k[x, y]/\langle x, y^2\rangle \times_k k[x, y]/\langle x^2, y\rangle$.

Theorem 6. *Let $(R, \mathfrak{m})$ be a local ring. Then $\mathfrak{m} = I \oplus J$ for some ideals I, J of R. Then $R \cong R/I \times_{R/\mathfrak{m}} R/J$ where the maps $f : R/I \to R/\mathfrak{m}$ and $g : R/J \to R/\mathfrak{m}$ are the natural quotient maps by $\mathfrak{m}/I$ and $\mathfrak{m}/J$ respectively.*

4 Localization

Whenever k is a field, the ring $k[[x]]$ has the property that its only non-zero prime ideal is $\langle x\rangle$. We can construct a similar ring staring with $\mathbb{Z}$ as well:

Theorem 7. *Let p be any prime number. Then there exists an integral domain R containing $\mathbb{Z}$ as a subring such that the only non-trivial prime ideal in R is $\langle p\rangle$. Moreover, all the non-zero ideals in R have the form $\langle p^n\rangle$ for some non-negative integer n.*

Proof. Let R be the set of rational numbers that have denominator not divisible by p (when written in the lowest terms). It is clear that this is an integral domain that contains $\mathbb{Z}$ as its subring. We use the concept of v_p for rational numbers. Since $v_p(x) \geq 0$ for all $x \in R$, for any non-zero ideal I we can choose a non-zero $x \in I$ with the smallest v_p value. Since any rational number with denominator not divisible by p is invertible in R, if $v_p(x) = n$, then we must have $p^n \in I$. Now since every other number in I has v_p at least n, it is a multiple of p^n in R, and so $I = \langle p^n\rangle$. □

We can do a similar thing for any integral domain:

Theorem 8. *Let R be an integral domain, and let I be any non-zero prime ideal of R. Then there exists an integral domain S containing R such that the ideal generated by elements of I in S is the unique maximal ideal of S.*

Proof. Let K be the field of fractions of R, and let S be the set of elements of K that contain an ordered pair (a,b) such that $b \in R \setminus I$. Since I is prime, the set $R \setminus I$ is closed under multiplication. Therefore it can be seen that S is closed under addition and multiplication, and hence is a subring of the field $K \implies S$ is an integral domain. Also, R can be embedded in S by $r \to [(r,1)]$ for all r, since $1 \in R \setminus I$. We denote the ideal generated by elements of I in S as I itself. Now assume J is any ideal in S, and let $a \in J$ be arbitrary. Suppose $(b,c) \in a$ where $c \in R \setminus I$. If $b \in I$, then clearly $a = b \cdot [(1,c)] \in I$. But if $b \notin I$, then a is a unit because $a \cdot [(c,b)] = 1$ in S, contradiction! Therefore we must have $J \subset I$. Thus I is the unique maximal ideal of S. □

The above process can be generalized.

Definition (Multiplicatively Closed Subset)**.** A subset A of a ring R is called multiplicatively closed if it satisfies the following properties:

1. $1 \in A$
2. $0 \notin A$
3. $ab \in A$ for all $a, b \in A$

Let R be a commutative ring and A be a multiplicatively closed subset. Consider the set $R \times A$. We define an equivalence relation on the set as follows: $(a,b) \sim (c,d)$ iff there are $x, y \in A$ such that $ax = cy$ and $bx = dy$. (Note that of $ad = bc$, this condition is obviously satisfied with $x = d$ and $y = b$.) This clearly satisfies symmetry and reflexivity, now let's look at transitivity. Assume $(a_1,b_1) \sim (a_2,b_2)$ and $(a_2,b_2) \sim (a_3,b_3)$. Then there are $x_1, y_1, x_2, y_2 \in A$ such that $a_1x_1 = a_2y_1$, $b_1x_1 = b_2y_1$, $a_2x_2 = a_3y_2$, and $b_2x_2 = b_3y_2$. But then $a_1x_1x_2 = a_2y_1x_2 = a_3y_1y_2$, and $b_1x_2x_2 = b_2y_1x_2 = b_3y_1y_2$, and hence $(a_1,b_1) \sim (a_3,b_3)$. Thus we can look at the set of equivalence classes, and induce it with addition and multiplication:

$$[(a,b)] \cdot [(c,d)] = [(ac,bd)]$$

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)]$$

We show that these are well-defined.

Suppose $(a_1,b_1) \sim (a_2,b_2)$ and $(c_1,d_1) \sim (c_2,d_2)$ with $a_1x_1 = a_2y_1$, $b_1x_1 = b_2y_1$, $c_1x_2 = c_2y_2$, and $d_1x_2 = d_2y_2$. Then note that we have $(a_1c_1)x_1x_2 = (a_2c_2)y_1y_2$ and $(b_1d_1)x_1x_2 = (b_2d_2)y_1y_2$, thus $(a_1c_1, b_1d_1) \sim (a_2c_2, b_2d_2)$, and so multiplication is well-defined.

Now note that $(a_1d_1 + b_1c_1)x_1x_2 = (a_2d_2 + b_2c_2)y_1y_2$ and $(b_1d_1)x_1x_2 = (b_2d_2)y_1y_2$, and thus $(a_1d_1 + b_1c_1, b_1d_1) \sim (a_2d_2 + b_2c_2, b_2d_2)$, and so addition is also well defined.

Finally, note that we have the unit element $[(1,1)]$.

Another equivalent way to define $\sim$ is the following: $(a,b) \sim (c,d)$ iff there is an $x \in A$ such that $(ad - bc)x = 0$.

We call the new ring thus defined the localization of R w.r.t. A, and denote is by $A^{-1}R$ Note that we can find a homomorphism from R in $A^{-1}R$: $r \to [(r,1)]$. This is clearly a homomorphism, and is injective in the case R is an integral domain: If $(r,1) \sim (s,1)$, then there are $x, y \in A$ such that $rx = sy$ and $x = y \implies rx = sx \implies r = s$ since $x \neq 0$. However even in the case that R is not an integral domain, the kernel of this homomorphism is the set of all $r \in R$ such that $rx = 0$ for some $x \in A$. Note that this is an ideal: $rx = 0$ and $sy = 0$ implies $(r+s)xy = 0$. Therefore, the homomorphism is injective iff none of the elements of A are zero divisors. We denote this homomoprhism by ϕ_A

Localization is, in some sense, inverting a certain subset of R. Indeed, the homomorphic image of any $a \in A$ is $[(a,1)]$, which has an inverse $[(1,a)]$. To that end, the following is true:

Theorem 9. *Let R be a commutative ring, and let A be a multiplicative subset of the set of its units. Then $R \cong A^{-1}R$*

Proof. Since no unit is a zero divisor, the natural homomorphism from R to $A^{-1}R$ is injective. Now we also show that it is surjective. Indeed, for any $[(a,b)]$, since b is a unit there is a $c \in R$ such that $bc = 1$. Then we have $(a \cdot 1 - (ac) \cdot b) \cdot 1 = 0$, and therefore $(a,b) \sim (ac, 1)$, which lies in the image of the homomorphism. □

5 Ideals in Localizations

Theorem 10. *There is a one-to-one correspondence between ideals of $A^{-1}R$ and ideals I of R such that all elements of A are not zero divisors in R/I. The explicit correspondence one way is given by $I \subset R$ goes to the ideal of $A^{-1}R$ generated by $\phi_A(I)$, and the other way is given by J goes to $\phi_A^{-1}(J)$.*

Proof. Let $R' = \phi_A(R)$ in $A^{-1}R$. For any ideal $J \subset A^{-1}R$, look at $R' \cap J$. This is an ideal of R'; moreover it generates J because $\frac{a}{b} \in J \implies \frac{a}{1} = \frac{b}{1} \cdot \frac{a}{b} \in R' \cap J \implies \frac{a}{b} = \frac{1}{b} \cdot \frac{a}{1}$. Further if $\frac{as}{1} \in R' \cap J$ for some $s \in A$, then we must have $\frac{a}{1} \in R' \cap J$. Therefore if $R' \cap J$ lifts to I in R, we must have $as \in I$ for some $s \in A \implies a \in I$, i.e., elements of A are not zero divisors in R/I. This gives us one map from ideals of $A^{-1}R$ to ideals of R satisfying the property.

Conversely, if I is an ideal of R satisfying that property, and $I' = \phi_A(I)$ in R' (note that I contains the kernel of this homomorphism), it generates an ideal J of $A^{-1}R$. We can check that $I' = R' \cap J$ by direct calculation: every element of I is the "numerator" of a sum of the form $\frac{x_1 a_1}{y_1} + \cdots + \frac{x_n a_n}{y_n}$ for some $a_i \in I$, $x_i \in R$ and $y_i \in A$, and we can check that that is in I as well. Indeed, if the numerator of this expression is r, then

$$ry_1 y_2 \cdots y_n = x_1 y_2 \cdots y_n a_1 + x_2 y_1 y_3 \cdots y_n a_2 + \cdots + x_n y_1 \cdots y_{n-1} a_n \in I$$

and so $r \in I$ because I satisfies the property. This gives a map from from ideals of R satisfying the property to ideals of $A^{-1}R$.

Now we show that the two maps are inverses of each other. Indeed, for any ideal I of R, let J be the ideal of $A^{-1}R$ generated by elements of $\phi_A(I)$. Then $\phi_A(I) = R' \cap J$ by the above, so I is the lift of $R' \cap J$, which is the first map. Conversely, if J is an ideal of $A^{-1}R$, and I is the lift of $R' \cap J$, then $\phi_A(I) = R' \cap J$, which generates J as we have proved. Thus the correspondence is bijective. □

A consequence of the above proof is also the following:

Theorem 11. *Let I be an ideal of R which is generated by a set of n elements. Then the corresponding ideal I' in $A^{-1}R$ can also be generated by a set of n elements.*

The correspondence theorem becomes much clearer when looking at prime ideals:

Theorem 12. *There is a one-to-one correspondence between prime ideals of $A^{-1}R$ and prime ideals of R that are disjoint from A.*

Proof. It is clear that if $J \subset A^{-1}R$ is prime, then its corresponding image $I \subset R$ is also prime, and further, since no element of A is a zero divisor in R/I, I must be disjoint from A. Conversely, suppose I is a prime ideal disjoint from A, then since R/I is an integral domain, elements of A are not zero divisors there, so I satisfies the required property. □

It is clear from the above that maximal ideals of $A^{-1}R$ correspond to the maximal ideals of R disjoint from A.

A common type of localization is the following: Given a prime ideal $\mathfrak{p}$, the set $R \backslash \mathfrak{p}$ is multiplicatively closed. If we localize w.r.t. that set, we get a ring $R_\mathfrak{p}$.

Theorem 13. *$R_\mathfrak{p}$ is a local ring, and its unique maximal ideal is the image of $\mathfrak{p}$.*

Proof. Clearly $\mathfrak{p}$ is the unique maximal ideal that is disjoint from $R \setminus \mathfrak{p}$, so the result follows. □

We can define localization for modules as well:

Definition. Let R be a commutative ring, A be a multiplicatively closed subset, and M be an R-module. Then $A^{-1}M$ is the set of all fractions $\frac{x}{s}$ where $x \in M$ and $s \in A$ such that

$$\frac{x}{s} = \frac{y}{r} \iff \exists t \in A \text{ such that } t(rx - sy) = 0$$

Another way to write a (weaker form of) the correspondence theorem is to say: Any ideal of $A^{-1}R$ has the form $A^{-1}I$ for some ideal I of R. Indeed, $A^{-1}I$ is just the ideal of $A^{-1}R$ generated by $\phi_A(I)$.

6 Nilpotents and Reduced Rings

If R is commutative, then the set of nilpotent elements of R form an ideal. We call that ideal the nilradical of the ring. We will assume commutativity of rings in this section.

Definition. A ring is called reduced if it has no non-zero nilpotent elements.

Theorem 14. *Let R be a commutative ring, and I be any ideal. Let J be the nilradical of R. Then*

1. *If R/I is reduced then $J \subset I$.*
2. *R/I is reduced if $I = J$.*

Proof. Assume there is some $x \in J$ not in I. Then $x + I \neq 0$ in R/I, but $(x + I)^n = x^n + I = 0$, so R/I is not reduced. Now, assume $I = J$. Let $x + I \in R/I$ be nilpotent $\implies x^n + I = 0$ for some n $\implies x^n \in I = J \implies x^n$ is nilpotent $\implies x^{mn} = 0$ for some $m \implies x$ is nilpotent $\implies x \in J = I$ $\implies x + I = 0$, as required. □

The condition $I = J$ is not necessary. Consider $R = k[x]$ for some field k. The only nilpotent element is 0, and $\langle 0 \rangle \neq \langle x \rangle$, but $k[x]/\langle x \rangle$ is still reduced (because it is isomorphic to the field k itself).

The condition $J \subset I$ is not sufficient as well. Again consider $R = k[x]$ for some field k. Then the only nilpotent element in R is 0, and $\langle 0 \rangle \subset \langle x^2 \rangle$, but $k[x]/\langle x^2 \rangle$ is not reduced.

In fact, a necessary and sufficient condition can be found:

Theorem 15. *Let R be a commutative ring, and I be any ideal. Then R/I is reduced iff I is a radical ideal, i.e., $\sqrt{I} = I$*

Proof. R/I is reduced $\iff$ for any $x + I \neq 0$ in R/I, x is not nilpotent $\iff$ for any $x \notin I$, $x^n \notin I$ for any $n \geq 1$ $\iff$ $\sqrt{I}$ has no elements outside of I $\iff$ $I = \sqrt{I}$. □

A case to consider is nilpotents in $k[x]/\langle p(x) \rangle$ where k is any field, and p is any polynomial. A polynomial q is nilpotent $\iff$ $q^n = 0$ in $k[x]/\langle p(x) \rangle$ for some n $\iff$ $p \mid q^n$ in $k[x]$ for some n $\iff$ all roots of p in algebraic closure of k are also roots of q. Thus $k[x]/\langle p(x) \rangle$ is reduced iff $p \mid q$ for all such q, which happens iff p is squarefree. In a similar fashion, $\mathbb{Z}_n$ is reduced iff n is squarefree.

Theorem 16. *Let R be a commutative ring, with J being its nilradical. Then the nilradical of $R[x]$ is $J[x]$.*

Proof. Let I be the nilradical of $R[x]$. Since all monomials of the form ax^k where $a \in J$ are nilpotent, we get $J[x] \in I$. Conversely suppose a polynomial $f \in I$. Then $f^n = 0$ for some $n \implies f(0)^n = 0$ $\implies$ constant term of f is in J. But then $f(x) - f(0)$ is also in I, and therefor so is $\frac{f(x)-f(0)}{x}$, and the constant term of that is also in J, and so on. Thus all coefficients of f are in $J \implies f(x) \in J[x]$. Thus $I = J[x]$. □

Note that the second part of the above proof also works for power series, and so we get

Theorem 17. *Let R be a commutative ring, with J being its nilradical. Then the nilradical of $R[[x]]$ is contained in $J[[x]]$.*

However, the converse of the above is not true. Consider

$$R = k[x_0, x_1, x_2, \dots]/\langle x_0^2, x_1^3, x_2^4, \dots \rangle$$

where k is a field having characteristic 0. Consider the following element in $R[[t]]$: $f(t) = x_0 + x_1 t + x_2 t^2 + \cdots$. Since each x_i is nilpotent, $f \in J[[t]]$. But for any positive integer n, the coefficient of $t^{\frac{n(n+1)}{2}}$ in f^n contains the term $x_0 x_1 \dots x_n$, which is non-zero and can never be cancelled since characteristic of k is 0. Thus f^n is never 0, and f is not nilpotent.

The above example also shows that the nilradical may not be nilpotent, i.e., it is possible that $J^n \neq \langle 0 \rangle$ for any positive integer n.

However, we recover our original theorem if we assume that R is Noetherian.

Theorem 18. *Let R be a commutative Noetherian ring, with J being its nilradical. Then the nilradical of $R[[x]]$ is $J[[x]]$.*

Proof. Let I be the ideal of nilpotents in $R[[x]]$. We have proved one part, i.e., $I \subset J[[x]]$, so we just have to prove the other. Assume $f \in J[[x]]$. Let ideal generated by coefficients of f be finitely generated as $\langle a_1, a_2, \dots a_n \rangle$. By our initial assumption on f, its coefficients are all in J, so each $a_i \in J$. We can write every coefficient of f as a finite linear combination of the a_is, so we have $f = a_1 f_1 + a_2 f_2 + \cdots + a_n f_n$ for some $f_i \in R[[x]]$. But, each $a_i f_i \in I$ since $a_i \in J$, and thus $f \in I$. This gives $I = J[[x]]$, as required. □

As a concrete example, consider $\mathbb{Z}_n[x]$. An integer is nilpotent in $\mathbb{Z}_n$ if every prime dividing n also divides it. Thus $f(x) \in \mathbb{Z}_n[x]$ is nilpotent iff every prime dividing n also divides every coefficient of f.

We can also characterize the nilradical in terms of prime ideals:

Theorem 19. *The nilradical of a commutative ring R is precisely the intersection of all the prime ideals of R.*

Proof. Let J be the nilradical, and let I be any prime ideal. For any $a \in J$, we have $a^n = 0 \in I$ for some positive integer n, and so either $a \in I$ or $a^{n-1} \in I$; in any case $a^{n-1} \in I$. Continuing this, we get $a \in I$. Therefore J lies in the intersection of all prime ideals.

Conversely, assume that c is not nilpotent. We will construct a prime ideal that doesn't contain c. Let S denote the set of all numbers of the form c^n for some positive integer n. Consider ideals that are completely contained in $R \setminus S$. This collection is clearly non-empty, because $\langle 0 \rangle$ is there. By a standard application of Zorn's lemma, we see that this collection has a maximal element, say I. We claim that I is prime. Suppose FTSOC that $ab \in I$ but neither a nor b are in I. Then the ideal generated by $I \cup \{a\}$ contains an element of S, say c^n. Therefore $c^n - xa \in I$ for some $x \in R \implies bc^n - xab \in I \implies bc^n \in I$. Similarly, there is a positive integer m and a $y \in R$ such that $c^m - yb \in I \implies c^{m+n} - ybc^n \in I \implies c^{m+n} \in I$, which contradicts the definition of I. Thus I is prime, as required. □

The second part of the proof also shows the following:

Theorem 20. *Let S be a multiplicatively closed subset of R that doesn't contain* 0*, then there is a prime ideal of R that is disjoint from S.*

7 Units in Polynomial and Power Series Rings

Again we only consider commutative rings.

Before characterizing units in polynomials, we need a small lemma: If a is nilpotent and u is a unit, then $a+u$ is also a unit. Indeed, if $b = a+u$, and $a^n = 0$, then $(b-u)^n = 0$. Expanding this with binomial theorem, we get

$$b \cdot \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} b^{i-1} = u^n$$

which is a unit. Thus a multiple of b is a unit, and hence b is a unit as well.

Theorem 21. *Let R be a commutative ring. A polynomial*

$$f = a_0 + a_1 x + \cdots a_n x^n$$

in $R[x]$ is a unit iff a_0 is a unit and a_i is nilpotent for all $i > 0$.

Proof. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a unit, say $fg = 1$ where $g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$. Comparing constant terms, we get $a_0 b_0 = 1$, so $f(0) = a_0$ is a unit. If $n = 0$ we are done. Hence assume $n > 0$. Now we use induction on k to prove that $a_n^k b_{m-k} = 0$ for all $k \leq m$. Base case: $k = 0$ is done by comparing coefficient of x^{m+n} term. Now assume the fact is true for all $i < k \leq m$. Comparing coefficient of x^{m+n-k} (note that $m+n-k > 0$), we get

$$\sum_{i=0}^{k} a_{n-k+i} b_{m-i} = 0$$

Multiplying both sides by a_n^{k-1}, we get

$$\sum_{i=0}^{k-1} a_{n-k+i} a_n^{k-1} b_{m-i} + a_n^k b_{m-k} = 0$$

By induction hypothesis, all other terms are 0, so the only term that remains is $a_n^k b_{m-k} = 0$. Thus we are done by induction, and in particular we get $a_n^m b_0 = 0$. Now multiplication by a_0 gives $a_n^m = 0$, i.e., a_n is nilpotent. Thus $a_n x^n$ is nilpotent, and using the lemma we get that $f(x) - a_n x^n$ is a unit. Thus doing the same thing as above again and again, we get $a_{n-1}, a_{n-2}, \ldots a_1$ are all nilpotent, which proves one half of the theorem. The second half is easier: if constant term of f is a unit and every other term is nilpotent, then repeatedly applying the lemma gives us that f is a unit. □

As a concrete example, consider $\mathbb{Z}_n[x]$. A polynomial f is a unit iff $f(0)$ is relatively prime with n and every prime dividing n also divides every other coefficient of f. Another example to consider is $k[x]/\langle f(x) \rangle$ where k is a field and f is any polynomial. A polynomial g is a unit $\iff$ there is a polynomial h such that $gh = 1$ in $k[x]/\langle f(x) \rangle$ $\iff$ there are polynomials h, l such that $gh - fl = 1$ in $k[x]$ $\iff$ f, g are relatively prime due to Bezout's theorem.

Classifying units in power series rings is much easier; in fact we can do much more:

Theorem 22. *Let R be a (not necessarily commutative) ring. Then $f \in R[[x]]$ has a right (resp. left) inverse iff $f(0)$ has a right (resp. left) inverse in R.*

Proof. If f has a right inverse, then $fg = 1$ for some power series $g \implies f(0)g(0) = 1 \implies f(0)$ has a right inverse. Now conversely assume that $f(0)$ has a right inverse. Let $f(x) = a_0 + a_1 x + \cdots$ where $a_0 = f(0)$. We will construct a power series $g(x) = b_0 + b_1 x + \cdots$ which is the right inverse of f, by finding the coefficients b_i inductively. Base Case: Choose b_0 such that $a_0 b_0 = 1$. Suppose we have chosen b_i for each $i < k$, for some $k > 0$. Now choose b_k such that:

$$b_k = -\sum_{i=0}^{k-1} b_0 a_{k-i} b_i$$

We can see by direct expansion that $fg = 1$, and we are done. □

In view of the lemma, we can consider the set of all a such that $1 + ra$ is a unit for all $r \in R$. We have the following result:

Theorem 23. *Let R be a commutative ring, and let I be the set of all $a \in R$ such that $1 + ra$ is a unit for all $r \in R$. Then I is an ideal; in fact it is exactly the intersection of all maximal ideals of R.*

Proof. Suppose $a \in I$. Let J be any maximal ideal of R. If $a \notin J$, then $a + J$ is invertible in the field R/J. Hence there is an r such that $(r + J)(a + J) = -1 \implies ra + 1 \in J$, which is impossible since it is a unit. Hence a is in every maximal ideal.

Conversely, assume a is in every maximal ideal. Assume FTSOC that $ra + 1$ is not a unit. Look at a maximal ideal containing $ra + 1$ (this exists due to Zorn's lemma). This maximal ideal contains a, and hence contains $ra + 1 - ra = 1$, conradiction! Hence $a \in I$, and we get the required theorem. □

The above ideal is called the Jacobson radical of R, and is denoted by $J(R)$.

8 Artinian and Noetherian Rings

Definition. A ring is called Artinian if every descending chain of ideals terminates.

In a non-commutative case, left-Artinian and right-Artinian conditions are there. Most rings are not Artinian: $\mathbb{Z}$ has the chain $\cdot \subset \langle 2^n \rangle \cdots \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle$. Polynomials and power series have $\cdot \subset \langle x^n \rangle \cdots \subset \langle x^2 \rangle \subset \langle x \rangle \subset \langle 1 \rangle$. Fields and finite rings are Artinian because they only have finitely many ideals. Here is a non-trivial example:

Theorem 24. *For any field k and positive integer n, $k[x]/\langle x^n \rangle$ is Artinian.*

Proof. Firstly, we note that $k[x]/\langle x^n \rangle \equiv k[[x]]/\langle x^n \rangle$. This is because in both cases, we are cutting the polynomial or power series at its x^n term. But every ideal in $k[[x]]$ is given by $\langle x^d \rangle$ for some non-negative integer d or $\langle 0 \rangle$, so the same must be true for $k[[x]]/\langle x^n \rangle$ as well. But for $d \geq n$, we have $x^d = 0$ in $k[[x]]/\langle x^n \rangle$. Thus the only ideals in $k[[x]]/\langle x^n \rangle$ are of the form $\langle x^d \rangle$ for $0 \leq d \leq n - 1$ and $\langle 0 \rangle$. Therefore R only has finitely many ideals, and so it is Artinian. □

This can be generalised by using the concept of k-algebras.

Definition (R-Algebra)**.** Let R be a commutative ring and S be an rng (ring possibly without unity). Suppose there is a ring homomorphism $\phi : R \to S$ whose image lies in the center of S. Then S is said to be an R-algebra.

Basically S acts like a module over R, but with a product as well. That product is associative and distributive on both sides. The scalar multiplication is defined as follows: $r \cdot s = \phi(r)s$ for all $r \in R$ and $s \in S$. The image being in the center allows $s(r \cdot t) = r \cdot (st)$

Theorem 25. *Let R be a ring and let k be a field. Suppose R is a k-algebra having finite dimension as a vector space over k. Then R is left-Artinian and left-Noetherian. In fact any strictly descending or ascending chain of left ideals has length at most* $\dim(R)$.

Proof. The key idea is to note that any left ideal of R is a vector subspace of R over k - this can be easily verified by the properties of left ideals.
Now assume $I \subset J \subset R$ are two left ideals, with $I \neq J$. If $\dim I = \dim J$, then since I is a subspace of J and they are finite dimensional, replacement theorem gives $I = J$, contradiction! Thus $\dim I < \dim J$. Taking $J = R$ as a special case gives $\dim I < \dim R$ for all proper left ideals I. These two inequalities immediately give the theorem as well as the bound, because any decreasing (resp. increasing) sequence of left ideals can be associated with a decreasing (resp. increasing) sequence of non-negative integers of size at most $\dim R$ via their dimensions. □

Clearly the above theorem also holds for right ideals.

The converse of the above theorem is not true: Clearly $\mathbb{R}$ is a $\mathbb{Q}$-algebra. Also, since $|\mathbb{R}|$ is uncountable and $|\mathbb{Q}|$ is countable, the dimension of $\mathbb{R}$ over $\mathbb{Q}$ as a vector space is infinite. Still, $\mathbb{R}$ is Artinian.

One application of the above theorem in a non-commutative case is matrices: For any field k the ring of square matrices $\mathcal{M}_n(k)$ is left-(and right-)Artinian for any positive integer n. This is because the ring can be written as a n^2 dimensional vector space over k. However I suspect that the bound of n^2 is weak, and that in fact every descending chain of left (or right) ideals in $\mathcal{M}_n(k)$ must have size at most n. However, in case of two-sided ideals, we have the following:

Theorem 26. *Let R be a ring. Then all the (two-sided) ideals in $\mathcal{M}_n(R)$ are of the form $\mathcal{M}_n(I)$ for some (two-sided) ideal I of R.*

Proof. Let $E_{i,j}$ denote the matrix with 1 in the (i,j) position and 0 everywhere else. For any ideal J of $\mathcal{M}_n(R)$, let I be the ideal generated by entries at $(1,1)$ position in matrices of J. This is indeed an ideal because of term-wise addition and multiplication (on both sides) by matrices of the form rI_n for any $r \in R$. For any matrix $A \in J$, we have

$$E_{1,i}AE_{j,1} = a_{i,j}E_{1,1} \in J$$

where $a_{i,j}$ is the (i,j) entry in A. Thus all entries in A are in I, and so $J \subset \mathcal{M}_n(I)$. Conversely, if $b \in \mathcal{M}_n(I)$ choose a matrix $B \in J$ with its $(1,1)$ entry being b. Then

$$E_{i,1}BE_{1,j} = bE_{i,j} \in J$$

and every matrix in $\mathcal{M}_n(I)$ can be written as a sum of such matrices. Thus $J = \mathcal{M}_n(I)$. □

In particular, the only ideals of $\mathcal{M}_n(k)$ are the zero ideal and the ring itself. This also proves that R is Artinian $\implies$ $\mathcal{M}_n(R)$ is Artinian.

The theorem also allows us to construct Artinian rings from polynomial rings with multiple variables. For example, $k[x,y]/\langle x^m, y^n\rangle$ is Artinian for any positive integers m, n.

Theorem 27. *Every left-(resp. right-)Artinian ring is left-(resp. right-)Noetherian.*

Proof. We will prove this result for commutative rings, later. □

Another way to construct Artinian rings is the following:

Theorem 28. *Let R be a commutative ring, and let M be a finitely generated maximal ideal of R. Then R/M^n is Artinian for any positive integer n.*

Proof. We use induction on n. Base Case: R/M is a field, so clearly Artinian. Note that M/M^n is the unique maximal ideal of R/M^n. This is because, for any maximal ideal $N \neq M$ of R, N contains an element a not in M, so $\langle a\rangle$ and M are comaximal $\implies$ $\langle a\rangle$ and M^n are comaximal, and so $N/M^n = R/M^n$. Therefore every proper ideal of R/M^n is contained in M/M^n. Now, note that we can embed $S = R/M^{n-1}$ into M/M^n via $x + M^{n-1} \to xM + M^n$. Also, we can define a scalar multiplication: $(x + M^{n-1}) \cdot (y + M^n) = xy + M^n$. Further, M^{n-1} is finitely generated since M is finitely generated. Therefore M/M^{n-1} is a finitely generated S-module, and since S can be embedded in M/M^n, any proper ideal of R/M^n is a submodule of M/M^n. We will prove later that any finitely generated module over an Artinian ring is Artinian, so in fact M/M^n is an Artinian module. This directly gives us that R/M^n is Artinian, as required. □

Theorem 29. *Let R be a commutative Artinian ring. Then,*

1. *Every prime ideal of R is maximal.*

2. There are only finitely many maximal ideals.

Proof. Assume first that there is a prime ideal I that is not maximal. Then R/I is an integral domain that is not a field. Moreover it is also Artinian. But then, there is an $a \in R/I$ which is not a unit, and so $\langle a \rangle \supset \langle a^2 \rangle \supset \cdots$ is an infinite decreasing sequence of ideals in R/I, contradiction!

Now assume there are infinitely many maximal ideals $M_1, M_2, \ldots$ in R. Then we get an infinite decreasing chain of ideals $M_1 \supset M_1M_2 \supset M_1M_2M_3 \supset \cdots$, contradiction! □

Here is another way to construct Artinian and Noetherian rings:

Theorem 30. *Product of any two Noetherian (resp. Artinian) rings is Noetherian (resp. Artinian).*

Proof. We'll prove this for the Noetherian case, since Artinian is similar. Let R, S be the two Noetherian rings. Let $I_1 \subset I_2 \subset \cdots$ be an increasing sequence of ideals of $R \times S$. Then $I_1 \cap (R, 0) \subset I_2 \cap (R, 0) \subset \cdots$ and $(I_1 + (R, 0))/(R,) \subset (I_2 + (R, 0))/(R, 0) \subset \cdots$ are increasing sequences of ideals of R, S respectively. Basically, the first sequence is like taking the elements r with $(r, 0) \in I_j$, and the second is just the projection of I_j to the second term. Therefore both of them are eventually constant. Choose a large n, and suppose there is an $x \in I_{n+1}$ that is not in I_n. From the second sequence being constant, there must be a $y \in (R, 0)$ such that $x + y \in I_n \subset I_{n+1}$. Hence $y \in I_{n+1} \cap L = I_n \cap L$, and hence we get $x \in I_n$, contradiction! Hence the sequence is eventually constant, and so M is Noetherian. □

Finally, Noetherianness can be passed onto polynomial rings:

Theorem 31 (Hilbert's Basis Theorem)**.** *Let R be a left-(resp. right-)Noetherian ring. Then $R[x]$ is left-(resp. right-)Noetherian.*

9 Prime Ideals in Noetherian Rings

We only look at commutative rings in this section.

We can give a nice characterisation of Noetherian rings in terms of prime ideals.

Theorem 32 (Cohen's Theorem)**.** *A commutative ring R is Noetherian iff any prime ideal of R is finitely generated.*

Proof. One direction is obvious, so assume every prime ideal of R is finitely generated. Consider the set of all ideals that cannot be finitely generated. This set satisfies the Zorn's property: for any chain I_j, the union of I_j cannot be finitely generated (else all the generators lie in one of the I_j, and hence generate that I_j). Therefore every chain has a maximal element, and so there is a maximal non-finitely generated ideal I.

We claim that I is prime. Indeed, FTSOC assume there exists $a, b \notin I$ such that $ab \in I$. Since I is strictly contained in $I + \langle a \rangle$, the latter is finitely generated, say by $c_1, c_2, \ldots c_n$. Let $r_1, r_2, \ldots r_n \in I$ be such that $c_i - r_i \in \langle a \rangle$. Also consider the ideal of all elements d such that $ad \in I$. This strictly contains I, because it contains $b \notin I$. Hence this can also be finitely generated, say by $d_1, d_2, \ldots d_m$. We claim that I is generated by $r_1, r_2, \ldots r_n, ad_1, ad_2, \ldots ad_m$. Indeed, we can write any $s \in I \subset I + \langle a \rangle$ as a linear combination of the c_i, so it can be written as a linear combination of the r_i plus some multiple al of a. Since each $r_i \in I$, we must have $al \in I$, and so al can be written as a linear combination of the ad_i. Hence the claim follows, and this immediately gives a contradiction as I cannot be finitely generated. □

We can use Cohen's theorem to prove the following:

Theorem 33. *Let R be a Noetherian ring. Then $R[[x]]$ is Noetherian.*

Proof. Let $\mathfrak{p}$ be a prime ideal in $R[[x]]$. Consider the ideal formed by the constant terms of elements of $\mathfrak{p}$. This ideal is finitely generated, say by $f_1(0), f_2(0), \dots f_n(0)$ for $f_i \in \mathfrak{p}$. We have two cases: $x \in \mathfrak{p}$ or $x \notin \mathfrak{p}$.

If $x \in \mathfrak{p}$, then $\mathfrak{p}$ can be generated by the f_i and x (because constant term can be fixed by the a_i and the rest can be handled by x), so it is finitely generated.

Now suppose $x \notin \mathfrak{p}$. Let $g_0 \in \mathfrak{p}$. Then there exist $a_{0,i} \in R$ such that g_0 and $\sum a_{0,i} f_i$ have the same constant term, so their difference is of the form xg_1. Since $x \notin \mathfrak{p}$, we must $g_1 \in \mathfrak{p}$, so we get $a_{1,i} \in R$ such that xg_1 and $\sum a_{1,i} x f_i$ have the same x term. So their difference has the form $x^2 g_2$, where again $g_2 \in \mathfrak{p}$. If we keep doing this, we end up with

$$g_0 = \sum (a_{0,i} + a_{1,i} x + a_{2,i} x^2 + \cdots) f_i \in \langle f_1, f_2, \dots f_n \rangle$$

Hence $\mathfrak{p}$ is generated by the f_i, and hence is finitely generated.

Therefore every prime ideal in $R[[x]]$ is finitely generated, and hence it is Noetherian. □

Prime ideals in Noetherian rings do have interesting properties.

Theorem 34. *Any proper radical ideal in a Noetherian ring can be written as a finite intersection of prime ideals.*

Proof. Assume FTSOC that some Noetherian ring R contains a radical ideal which cannot be written as a finite intersection of prime ideals. Since R is Noetherian, there exists a maximal radical ideal I which cannot be written as a finite intersection of prime ideals. Therefore I cannot be prime, so there exist $x, y \notin I$ such that $xy \in I$. Note that $[I : x]$ is a radical ideal. Indeed, $z^m \in [I : x] \implies xz^m \in I \implies x^m z^m = (xz)^m \in I \implies xz \in I \implies z \in [I : x]$, as required. Further, $I \subsetneq [I : x]$ because $y \in [I : x]$ but $y \notin I$. Therefore, $[I : x]$ can be written as a finite intersection of prime ideals.

Now consider $J = \sqrt{I + \langle x \rangle}$. Again, $I \subsetneq J$ because $x \in J$ but $x \notin I$. Thus J, also being a radical ideal, can be written as a finite intersection of prime ideals as well.

It is clear that $I \subset J \cap [I : x]$. Let $t \in J \cap [I : x]$ be arbitrary. Then, $t \in J \implies t^m - ax \in I$ for some $a \in R$ and $m \in \mathbb{N} \implies xt^m - ax^2 \in I \implies -ax^2 \in I$ since $xt \in i \implies a^2x^2 = (ax)^2 \in I \implies ax \in I \implies t^m \in I \implies t \in I$. Thus in fact $I = J \cap [I : x]$, and so can also be written as a finite intersection of prime ideals, contradiction! □

Using the above theorem, we can prove a result about minimal primes in Noetherian rings.

Definition. A prime ideal of a ring is called a minimal prime ideal if it doesn't strictly contain any prime ideals of the ring.

Theorem 35. *Any prime ideal of a ring contains a minimal prime ideal.*

Proof. Let I be a prime ideal of a ring R. Consider the set S of all prime ideals contained in I. Suppose we have a descending chain $J_1 \supset J_2 \supset \cdots$ of elements of S, then this chain has a lower bound: the intersection of all the J_i. Thus by Zorn's lemma, this collection has a minimal element, as required. □

Theorem 36. *The nilradical of any Noetherian ring is nilpotent.*

Proof. Suppose the nilradical $\mathrm{Nil}(R)$ of a Noetherian ring R is generated by elements $\{x_1, \cdots x_k\}$, and suppose $x_i^{n_i} = 0$ for all i. Choose an $n > n_1 + n_2 + \cdots + n_k$. We can see that all generators of $\mathrm{Nil}(R)^n$ turn out to be 0, so $\mathrm{Nil}(R)^n = 0$, as required. □

Theorem 37. *Any Noetherian ring has only finitely many minimal prime ideals.*

Proof. Since the nilradical $\mathrm{Nil}(R)$ is a radical ideal, there exist finitely many prime ideals $\mathfrak{p}'_1, \dots \mathfrak{p}'_k$ such that $\mathrm{Nil}(R) = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_k$. For each i, choose a minimal prime ideal $\mathfrak{p}_i \subset \mathfrak{p}'_i$. Then since $\mathrm{Nil}(R)$ is the intersection of all prime ideals in R, we have

$$\mathrm{Nil}(R) = \mathfrak{p}'_1 \cap \cdots \cap \mathfrak{p}'_k \supset \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \supset \mathrm{Nil}(R)$$

$\implies$ $\mathrm{Nil}(R) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$. We claim that $\mathfrak{p}_i$ are the only minimal prime ideals in R, which would prove our statement. Indeed, assume there is some minimal prime ideal $\mathfrak{p}_{k+1} \neq \mathfrak{p}_i$ for all $i \leq k$. Since R is Noetherian, there exists an n such that $\mathrm{Nil}(R)^n = 0$. Therefore $(\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k)^n \subset \mathrm{Nil}(R)^n = 0$ $\implies$ $(\mathfrak{p}_1 \cdots \mathfrak{p}_k)^n = 0$. Since $\mathfrak{p}_{k+1}$ is also prime, we must have $\mathfrak{p}_i \subset \mathfrak{p}_{k+1}$ for some $i \leq k$. But this is impossible because $\mathfrak{p}_{k+1}$ is a minimal prime. □

10 Introduction to Modules

Definition (Module)**.** A module over a ring R is an abelian group M along with a scalar multiplication function $\cdot : R \times M \to M$ satisfying the same axioms as scalar multiplication for vector spaces:

1. $r \cdot (x + y) = r \cdot x + r \cdot y$
2. $(r + s) \cdot x = r \cdot x + s \cdot x$
3. $r \cdot (s \cdot x) = (rs) \cdot x$
4. $1 \cdot x = x$

The last axiom is there to ensure that everything does not go to 0.

Which properties of vector spaces carry over to modules?

1. Uniqueness of additive identity.
   Also holds for modules because the underlying structure is still an abelian group.

2. Uniqueness of additive inverse.
   Also holds for modules because the underlying structure is still an abelian group.

3. $0 \cdot v = 0 \ \forall v \in M$
   Also holds for modules. We have

$$0 \cdot v + 0 \cdot v = (0 + 0) \cdot v = 0 \cdot v$$

$$\implies 0 \cdot v = 0$$

4. $r \cdot 0 = 0 \ \forall r \in R$
   Also holds for modules. We have

$$r \cdot 0 + r \cdot 0 = r \cdot (0 + 0) = r \cdot 0$$

$$\implies r \cdot 0 = 0$$

5. $(-1) \cdot v = -v \ \forall v \in M$
   Also holds for modules. Note that we have $1 \cdot v = v$, so

$$v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0$$

$$\implies (-1) \cdot v = -v$$

6. $r \cdot v = 0 \implies r = 0$ or $v = 0$.
This may not hold for modules in general. For example, consider $\mathbb{Z}_4$ as a module over itself, with scalar multiplication being the usual multiplication. We have $2 \cdot 2 = 4 = 0$, but $2 \neq 0$.

In fact, Property (6) rarely holds:

Theorem 38. *Let R be a ring. Then Property (6) holds for all modules over R iff R is a skew field.*

Proof. First assume R is skew field. Then for any $r \in R$, if $r \neq 0$ there is an $s \in R$ with $sr = 1$, so $r \cdot v = 0$ and $r \neq 0 \implies (sr) \cdot v = s \cdot (r \cdot v) = 0 \implies 1 \cdot v = v = 0$. Therefore Property (6) holds for all modules over R.

Now suppose R is not a skew field. Suppose $a \in R$ is a non-zero element which doesn't have a left inverse, and so $I = Ra$ is a proper left ideal. Then I can be thought of as a module over R, and hence we can talk about the quotient R/I as a module over R. Addition is defined in the obvious manner, and multiplication is defined as $r \cdot (b + I) = rb + I$. Then note that $a \cdot (1 + I) = a + I = 0$ in R/I. Clearly $a \neq 0$ in R. Also, since I is a proper left ideal, $1 \notin I \implies 1 + I \neq 0$. Thus we have found a required counterexample.

Therefore every element in R has a left inverse. Let $a \in R$ be arbitrary, and let b be the left inverse of a, and let c be the left inverse of b. Then

$$a = (cb)a = c(ba) = c$$

Hence $ab = ba = 1$, and a is a unit. Therefore all elements of R are units, and so R is a skew field. □

In the case of commutative rings, Property (6) holds for all modules over R iff R is a field.

Note that R is a module over itself, and all ideals of R are precisely the submodules of R.

If M is an R-module, then we can ask whether it is a R/I-module for any ideal I in a sensible way. What we mean by that is, is there a scalar product $\cdot : R/I \times M \to M$ such that $(r + I) \cdot x = r \cdot x$ for all $r \in R$ and $x \in M$. This is false in general: $\mathbb{Z}$ is a $\mathbb{Z}$-module, but is not a $\mathbb{Z}/2\mathbb{Z}$-module because $2 \cdot 1 = 1 + 1 = 2 \neq 0$, while $2 = 0$ in $\mathbb{Z}/2\mathbb{Z}$. In fact, if M is a R module as well as R/I module under standard scalar multiplication, then we must have $rm = 0 \cdot m = 0$ for any $r \in I$. Therefore $IM = 0$. Conversely, if $IM = 0$, then we can define a product $(r + I) \cdot m = r \cdot m$, which characterizes M as a R/I-module.

Definition. The annihilator of an R-module M is the set of all $r \in R$ such that $rx = 0$ for all $x \in M$, and is denoted by $\mathrm{Ann}_R(M)$. This set forms a left-ideal of R. A module is called faithful iff its annihilator is the zero ideal.

Therefore another equivalent characterization is this: An R-module M is an R/I-module iff I is a subset of the annihilator of M. In other cases, we can still look at the submodule $N = IM$, i.e., set of elements of the form rm where $m \in M$ and $r \in I$. Now we look at the module M/N. Clearly this module satisfies $I(M/N) = 0$, and so is a R/I-module.

Another question we can ask is, if A is multiplicatively closed subset of R, then when is an R-module M also an $A^{-1}R$ module? Again the product must naturally extend like $\frac{r}{1} \cdot x = r \cdot x$. Then for any $x \in M$ and $s \in A$, we have

$$x = s \cdot \frac{1}{s} \cdot m = s \cdot y$$

for some $n \in M$. Thus, in some way, M is "divisible" by S. Further, $s \cdot y = 0 \implies y = \frac{1}{s} \cdot s \cdot y = 0$, so the division in "unique". Conversely, if division by A exists and is unique in M, then we can define $\frac{r}{s} \cdot x = r \cdot \frac{x}{s}$. We can check that this is well-defined: If $\frac{r}{s} = \frac{r'}{s'}$, then $s'r - rs'$ is annihilated by some element of A, and so $(s'r - rs') \cdot x = 0$ (because we can uniquely divide by elements of A). Therefore by expanding and dividing, we get $r \cdot \frac{x}{s} = r' \cdot \frac{x}{s'}$, as required.

Another way to say this is: M is an $A^{-1}R$-module iff for every $r \in A$, multiplication by r is an isomorphism of M.

Now in other cases, we can still create an $A^{-1}R$ module. Indeed, just look at $A^{-1}M$. This is because we can define multiplication as:

$$\frac{a}{r} \cdot \frac{x}{s} = \frac{ax}{rs}$$

Another question to ask is: what are the submodules of $A^{-1}M$?

Theorem 39. *The submodules of $A^{-1}M$ have the form $A^{-1}N$ for some $N \subset M$*

Proof. Let N' be a submodule of $A^{-1}M$. Let N be the set of numerators of N', i.e., the set of all x such that $\frac{x}{s} \in N'$ for some $s \in A$. This is clearly a submodule of M because for any $a, b \in R$ and $x, y \in N$, there exist $r, s \in A$ such that $\frac{x}{r}, \frac{y}{s} \in N'$, and this implies:

$$\frac{ax + by}{rs} = \frac{a}{s} \cdot \frac{x}{r} + \frac{b}{r} \cdot \frac{y}{s} \in N'$$

$\implies ax + by \in N$, as required. Then it is clear that $N' = A^{-1}N$. □

We can also consider the annihilators of submodules of M. For example, for any $x \in M$, look at $\mathrm{Ann}_R(x)$. This is an ideal of R, but is it always prime for some $x \in M$?

Theorem 40. *Let R be a Noetherian commutative ring, and let M be a non-zero R-module. Then there exists a prime ideal I such that $\mathrm{Ann}_R(x) = I$ for some $x \in M$.*

Proof. Consider the set of all proper ideals of the form $\mathrm{Ann}_R(x)$ for some $x \in M$. Then every chain in this set has a maximal element, because R is Noetherian. Therefore this set has a maximal element, say I. We claim that I is prime. Indeed, assume $ab \in I$, and WLOG $b \notin I$. If $I = \mathrm{Ann}_R(y)$, then $I + \langle a \rangle$ annihilates $by \neq 0$, and so we must have $a \in I$, as required. □

11 Modules over $\mathbb{Z}$

We begin by noting that $\mathbb{Z}$-modules are precisely abelian groups: indeed, multiplication by an integer is the same as repeated addition. Therefore any rng can be thought of as a $\mathbb{Z}$-module by virtue of its underlying abelian group. Also, any ring can be thought of as a $\mathbb{Z}$-algebra by virtue of the homomorphism $n \to n \cdot 1$.

Definition. Let R be a ring, and let $\phi : \mathbb{Z} \to R$ be the homomorphism given by $\phi(n) = n \cdot 1$ for all integers n. Suppose $\ker(\phi)$ is generated by $d \geq 0$ (such a d exists because $\ker(\phi)$ is an ideal of $\mathbb{Z}$, which is a PID). Then this d is called the characteristic of the ring R, and is denoted by $\mathrm{char}(R)$

Clearly if $\mathrm{char}(R) = n$, then $n \cdot r = 0$ for all $r \in R$, because $n \cdot 1 = 0$.

Theorem 41. *Let R be a domain. Then $\mathrm{char}(R)$ is either 0 or a prime number.*

Proof. Assume that $\mathrm{char}(R) = n > 0$. Let ϕ be the homomorphism as defined above. Then note that $\mathrm{Im}(\phi)$ is a subring of R, and hence is also a domain. However by the first isomorphism theorem, $\mathrm{Im}(\phi) \cong \mathbb{Z}/n\mathbb{Z}$, which is a domain only if n is a prime, and we are done. □

Theorem 42. *Let R be a local commutative ring. The $\mathrm{char}(R)$ is either 0 or a power of a prime.*

Proof. Suppose $\mathrm{char}(R) = n \neq 0$. Let $\mathfrak{m}$ be the unique maximal ideal of R. Suppose p is a prime factor of n. Let I_p be the set of all $r \in R$ such that $\frac{n}{p} \cdot r = 0$. Clearly I_p is an ideal of R. Suppose n has another prime factor q, then we can construct I_q as an ideal as well. $I_p \subset \mathfrak{m}$ and $I_q \subset \mathfrak{m} \implies I_p + I_q \subset \mathfrak{m}$ is a proper ideal. However, $p \in I_p$ and $q \in I_q$, and since p, q are distinct primes, there exist positive integers m, l such that $mp - lq = 1 \in I_p + I_q$, contradiction! □

Suppose we have an rng R. We can create a new ring containing R that retains many properties of R. The underlying set is $\mathbb{Z} \times R$, with addition defined term-wise. Product is defined as follows:

$$(m, a) \cdot (n, b) = (mn, na + mb + ab)$$

Basically the product can be thought of as expanding $(m + a) \cdot (n + b)$. This creates a new ring R', because it has the unit $(1, 0)$. We can embed R into R' via the homomorphism $r \to (0, r)$. In fact, R is an ideal of R': $(m, a) \cdot (0, r) = (0, mr + ar) \in R$ and $(0, r) \cdot (m, a) = (0, mr + ra) \in R$. Therefore we can concern ourselves with only rings (with unity).

We can generalize this construction. Suppose we have a commutative ring R and a module M, with some sort of multiplication $\cdot : M \times M \to M$ defined. Then we can get a similar structure on $R \times M$. When is this a ring? The underlying structure is definitely an abelian group because it is a product of two abelian groups. We need to check associativity:

$$(r, a) \cdot ((s, b) \cdot (t, c)) = (r, a) \cdot (st, sc + tb + b \cdot c) = (rst, rsc + rtb + sta + r(b \cdot c) + a \cdot (sc) + a \cdot (tb) + a \cdot (b \cdot c))$$

$$((r, a) \cdot (s, b)) \cdot (t, c) = (rs, sa + rb + a \cdot b) \cdot (t, c) = (rst, rsc + rtb + sta + (rb) \cdot c + (sa) \cdot c + t(a \cdot b) + (a \cdot b) \cdot c))$$

Thus we must have $\cdot$ is associative, and $(ra) \cdot b = a \cdot (rb) = r(a \cdot b)$. We must also check distributivity:

$$(r, a) \cdot ((s, b) + (t, c)) = (r, a) \cdot (s + t, b + c) = (rs + rt, rb + rc + sa + ta + a \cdot (b + c))$$

$$(r, a) \cdot (s, b) + (r, a) \cdot (t, c) = (rs, rb + sa + a \cdot b), (rt, rc + ta + a \cdot c) = (rs + rt, rb + rc + sa + ta + a \cdot b + a \cdot c)$$

Thus the product is left distributive, and similarly it must be right distributive as well. Therefore M must have an R-algebra-like structure (but maybe without unity). We can check that this condition is sufficient, because again we have unity $(1, 0)$. Also this ring is commutative iff the product on M is commutative.

A special case is when the product on M satisfies $a \cdot b = 0$ for all $a, b \in M$. In this case, the ring we have constructed is precisely the ring of all matrices of the form $\begin{bmatrix} r & a \\ 0 & r \end{bmatrix}$ for $r \in R$ and $a \in M$, with usual matrix addition and multiplication. This ring is called the idealization of M w.r.t. R.

12 Ideals in Idealization

Suppose M is an R-module, and S is its idealization. Then as above, we can prove that M is in fact an ideal of S, which satisfies $M^2 = 0$. In particular, since M annihilates itself, M is also an S/M-module. But note that $S/M \cong R$. These two interpretations of M as a module are in fact the same, because

$$((s, y) + M) \cdot (0, x) = (s, y) \cdot (0, x) = (0, sx) = s \cdot (0, x)$$

We can say something more about ideals of S:

Theorem 43. *Sets of the form $I \times N$ where I is an ideal of R and N is a submodule of M are ideals of S iff $IM \subset N$.*

Proof. Let $J = I \times N$ be an ideal of S, and let $(r, x) \in J$. Note that $(r, x) \cdot (0, y) = (0, ry) \in J$. Therefore we must have $IM \subset N$. Conversely, if this is true, then for any $(r, x) \in I \times N$, we have $(r, x) \cdot (s, y) = (rs, sx + ry) \in I \times N$ because $ry \in N$ for any $y \in M$. Hence $I \times N$ is an ideal of S. □

Theorem 44. *Let J be an ideal of S. Then $(\pi_1(J)^2, 0) \subset J$ and $(0, \pi_1(J)\pi_2(J)) \subset J$*

Proof. Let $\pi_1(J) = I$ and $\pi_2(J) = N$. Note that $(a, x) \in J \implies (0, ay) = (0, y) \cdot (a, x) \in J$, and so $(0, IM) \subset J$. Further, $(a, x) \cdot (a, -x) = (a^2, 0) \in J$, and so $(I^2, 0) \subset J$, as required. □

This is enough to derive information about maximal, prime and radical ideals in S:

Theorem 45. *The maximal ideals of S are of the form $I \times M$ where I is a maximal ideal of R.*

Proof. Let J be a maximal ideal of S, and let I be the set of all $r \in R$ such that $(r, x) \in J$ for some $x \in M$. Then clearly $J \subset I \times M$, so either $J = I \times M$ or $I = R$. In the former case, I is clearly maximal, because otherwise we can embed J in $I' \times M$ for some ideal I' strictly containing I. In the latter case, we have $(1, x) \in J$ for some $x \implies (1, x) \cdot (0, y) = (0, y) \in J$ for all $y \in M$. Therefore $(1, y) \in J$ for all $y \in M$, and so $(r, 0) \cdot (1, y) - (0, (r-1)y) = (r, y) \in J$ for all $r \in R$ and $y \in M$. This gives $J = S$, contradiction!

Conversely, assume $J = I \times M$ where I is maximal. Then we can directly check that $S/J \cong R/I$ is a field, and we are done. □

Theorem 46. *The prime ideals of S are of the form $I \times M$ where I is a prime ideal of R.*

Proof. Assume J is a prime ideal of S. Let $I = \pi_1(J)$. Then $(a, x) \in S \implies (a, x) \cdot (a, -x) = (a^2, 0) = (a, 0) \cdot (a, 0) \in J$. Since J is a prime ideal, we must have $(a, 0) \in J$, and so $(I, 0) \in J$. This clearly gives $J = I \times N$ for some submodule N. By the above, we have $IM \subset N$, so for any $a \in I$ and $y \in M$, we have $(0, ay) = (a, y) \cdot (0, y) \in J$, and so either $(a, y) \in J$ or $(0, y) \in J$; in any case $(0, y) \in J$. Thus $N = M$. Now, from $S/J \equiv R/I$, it is straightforward to show that I is prime. The converse also holds by the above isomoprhism. □

Theorem 47. *The radical ideals of S are of the form $I \times M$ where I is a radical ideal of R.*

Proof. Note that $(0, M)^2 = 0$, so for any radical ideal J, $(0, M) \in J$. Now it is easy to see that J has the form $I \times M$ for some ideal $I \subset R$. Then, $a^n \in I$ for some $n \implies (a^n, 0) \in J \implies (a, 0) \in J \implies a \in I$, so I is a radical ideal. The converse can be proved in the same way as the above two results. □

We can also say when S is Noetherian or Artinian:

Theorem 48. *The idealization S is Noetherian iff R is Noetherian and M is finitely generated.*

Proof. Assume S is Noetherian. Note that any submodule of M corresponds to an ideal of S, and so M is finitely generated (in fact it is Noetherian). Also, for any ideal $I \subset R$ we can correspond to it a unique ideal $I \times IM \subset S$, which has the same ascending conditions as I, and so R is also Noetherian.

Conversely, assume R is Noetherian and M is finitely generated. By Cohen's theorem, it is sufficient to prove that every prime ideal of S is finitely generated. However, every prime ideal of S has the form $I \times M$ for some prime ideal $I \subset R$, so it can clearly be finitely generated. □

Theorem 49. *The idealization S is Artinian iff R is Artinian and M is finitely generated.*

Proof. Assume S is Artinian $\iff$ S is Noetherian and all primes are maximal $\iff$ R is Noetherian, M is finitely generated, and all primes in R are maximal (this follows from characterization of prime and maximal ideals in S) $\iff$ R is Artinian and M is finitely generated. □

There is another way to prove that above two theorems. Note that we have a natural short exact sequence of S-modules $0 \to M \to S \to R \to 0$: we think of M as an ideal of S, and R as the quotient module S/M. Further, any S-submodule of R is an ideal of R and vice versa, since R can be thought of as an $S/M \equiv R$-module (because $MR = 0$). Also, the S-module M can be thought of as a $S/M \equiv R$ module as well because $M^2 = 0$. Therefore S is Noetherian (resp. Artinian) $\iff$ R, M are Noetherian (resp. Artinian) as S-modules $\iff$ R, M are Noetherian (resp. Artinian) as R-modules $\iff$ R is Noetherian (resp. Artinian) and M is finitely generated (here we used the fact that any Artinian module over an Artinian ring is finitely generated).

Theorem 50. *Let $Z(\cdot)$ denote the zero divisors of any ring or module (i.e. annihilator of a non-zero element of the module). Then $Z(M) \times M \subset Z(S)$. Equality holds if M is faithful.*

Proof. If $a \in Z(M)$, then there exists a $n \neq 0$ such that $an = 0$. This implies $(a,m) \cdot (0,n) = (0,0)$, so $(a,m) \in Z(S)$ for any $m \in M$.

Now assume $(a,m) \in Z(S) \implies (a,m) \cdot (b,n) = (ab, an + bm) = (0,0)$ where either $b \neq 0$ or $n \neq 0$. If $b = 0$, then $n \neq 0$ but $an = 0 \implies a \in Z(M)$, as required.

Assume $b \neq 0$, then $ab = 0$. If M is faithful, there exists an $x \in M$ such that $bx \neq 0$, but $a \cdot (bx) = 0 \implies a \in Z(M)$, as required. □

13 Basis for Modules

Definition. We say a subset $S \subset M$ is a generating set for an R-module M if every element in M can be written as a finite linear combination of elements from S.

If S is the generating set of M, we write $M = \langle S \rangle$ This is because if I is an ideal of R, then the generating sets of I as an ideal or as a module are the same.

Now we state a result that we've used in some form throughout the paper:

Theorem 51. *Let M be an R-module, and N be its submodule. Suppose M can be generated by a set of n generators for some positive integer n. Then M/N can be generated by a set of at most n generators.*

A way to use this is the following: Suppose we have a module homomorphism $\phi : M \to N$. Then note that $\mathrm{Im}(\phi)$ is a submodule of N and $\ker(\phi)$ is a submodule of M. Further we can check that

$$M/\ker(\phi) \cong \mathrm{Im}(\phi)$$

Therefore, if $\mathrm{Im}(\phi)$ can't be generated by less than n generators, then M also cannot be generated by less n generators.

Definition. We say a subset S of an R-module M is linearly independent if no non-trivial finite linear combination of elements of S is 0.

Definition. A basis of an R-Module is a linearly independent generating set.

Theorem 52. *A subset S of an R-module M is a basis iff every element in M can be uniquely written as a finite linear combination of elements from S.*

Proof. If very element in M can be uniquely written as a finite linear combination of elements from S, then 0 can be written uniquely as the empty sum, and hence S is linearly independent and therefore a basis. Conversely, if S is a basis, and an element in M can be written in two ways as a linear combination of elements of S, then we can subtract these representations to get a non-trivial linear combination that sums to 0, contradiction! □

Theorem 53. *Let R be a ring. Then every R-module has a basis iff R is a skew field.*

Proof. First assume R is not a skew field. Then from the proof of the theorem about Property (6), we get an R-module that does not satisfy Property (6). In fact, in that module $a \cdot v = 0$ for every $v \in M$. Thus such a module cannot have a basis, since even any singleton set is not linearly independent. Conversely, assume that R is a skew field, and M is an R-module. We claim that if S is any linearly independent set and v is not an element in the span of S, then $S \cup \{v\}$ is also linearly independent. The proof is the same as vector spaces. Now we can use Zorn's lemma to get a maximal independent set for M, which must form a basis. □

We can look at three equivalent definitions of a basis in the case of vector spaces:

1. Linearly independent generating set.

2. Minimal generating set.

3. Maximal linearly independent set.

These equivalences may not hold for modules. Indeed, look at $\mathbb{Z}$ as a $\mathbb{Z}$-module. The possible bases are $\{1\}$ and $\{-1\}$. However, any singleton set is a maximal linearly independent set, while there exist minimal generating sets of arbitrary size: Look at n different primes $p_1, p_2, \dots p_n$, and let P be the product of these primes, then the set $\{\frac{P}{p_1}, \dots \frac{P}{p_n}\}$ is a minimal generating set of size n.

However, things can get pretty bad if a module is not free. For example, in the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$, the only maximal linearly independent set is the empty set. Also in the $\mathbb{Z}$-module $\mathbb{Q}$, there is no minimal generating set. Indeed, if S is a generating set of $\mathbb{Q}$, and $a \in S$, then for any non-zero $b \in S$ with $b \neq a$ (such a b exists because $\frac{a}{2}$ cannot be generated by a alone), we can write $ma = nb$ for some integers m, n with $m \neq 0$. Hence $S \setminus \{a\}$ generates $ma \implies$ for any rational number x, $mx \in \langle S \setminus \{a\} \rangle$. But any rational number can be written as $m \cdot \frac{x}{m}$, and hence $\mathbb{Q}$ is generated by $S \setminus \{a\}$ as well. Therefore there cannot be a minimal generating set.

Definition. An R-module M is called finitely generated if it has a finite generating set.

A natural question to ask is, if M is finitely generated, then is every submodule of M also finitely generated? The answer is no in the general case. Let $R = k[x_1, x_2 \dots]$ where k is a field, and take $M = R$. Clearly M is finitely generated (in fact it is $\langle 1 \rangle$). However look at the submodule $\langle x_1, x_2, \dots \rangle$. Assume FTSOC that it is finitely generated, say by $f_1, f_2, \dots f_n$. However these polynomials only contain finitely many variables, so they are contained in $\langle x_1, x_2, \dots x_n \rangle$ for some positive integer n. But clearly we have x_{n+1} not in this ideal, contradiction! Thus this submodule is not finitely generated.

However, if we assume R is Noetherian, the statement is true.

Theorem 54. *Let R be a left-Noetherian ring, and let M be a finitely generated R-module. Then M is Noetherian.*

Proof. Suppose $M = \langle a_1, a_2, \dots a_n \rangle$. We will use induction on n to show that every submodule of M is finitely generated. If $n = 1$, then M is clearly isomorphic to R as a module, and so all submodules are left ideals of R, which are finitely generated since R is left-Noetherian. Now assume $n \geq 2$, and let N be a submodule of M. Let I be the set of all $r \in R$ such that $ra_1 \in N$. Since N is a module, I is a left ideal of R. Therefore it can be finitely generated, say by $\{b_1, b_2, \dots b_m\}$. Let $M' = \langle a_2, \dots a_n \rangle$, generated by $n-1$ elements. Let N' be the set of vectors y such that $ra_1 + y \in N$ for some $r \in R$. Clearly N' is a submodule of M', and hence by induction hypothesis is finitely generated, say by $y_1, y_2, \dots y_k$. Choose $c_1, c_2, \dots c_k \in R$ such that $c_i a_1 + y_i \in N$ for all i.

We claim that the finite set $\{b_1 a_1, \dots b_m a_1, c_1 a_1 + y_1, \dots c_k a_1 + y_k\}$ generates N. Indeed, assume $ra_1 + y \in N$. Then $y \in N'$, so it can be written as $r_1 y_1 + \cdots + r_k y_k$ for some $r_i \in R$. Now, subtracting $r_1(c_1 a_1 + y_1) + \cdots + r_k(c_k a_1 + y_k)$, we get $(r - r_1 c_1 - \cdots - r_k c_k) a_1 \in N$. Therefore $r - r_1 c_1 - \cdots - r_k c_k \in I$, which means it can be written as $s_1 b_1 + \cdots + s_m b_m$ for some $s_i \in R$. Combining these two, we get

$$ra_1 + y = s_1 b_1 a_1 + \cdots + s_m b_m a_1 + r_1(c_1 a_1 + y_1) + \cdots + r_k(c_k a_1 + y_k)$$

as the required linear combination. □

The above proof in fact proves the following: If every left ideal in R can be generated by at most m elements, and M is an R-module generated by n elements, then every submodule of M can be generated by at most mn elements.

Note that we can look at ideals of a ring as submodules, and ask when they have a basis.

Theorem 55. *Let R be a commutative ring, and let I be an ideal of R. Then I is a free R-module iff it is a principal ideal generated by a non-zero divisor of R.*

Proof. Clearly if $I = \langle a \rangle$ for some non-zero divisor a of R, then $\{a\}$ is a basis for I. Conversely, assume that I has a basis. Clearly no basis element can be a zero divisor, and if the basis has two elements a, b, then we have $a \cdot b + (-b) \cdot a = 0$, contradiction! □

Therefore every ideal of R has a basis iff R is a PID. This can be extended further:

Theorem 56. *Let R be a PID, and let n be a positive integer. Then any submodule of R^n is free.*

Proof. We use induction on n; in fact we prove that every basis has size at most n. $n = 1$ is proved above. Now assume the theorem is true for $n - 1$. Let M be a submodule of R^n. Let N' be the projection of M onto the first $n - 1$ entries. This is a submodule of R^{n-1}, so it has a basis of size at most $n - 1$, say $v'_1, v'_2, \dots v'_k$. Suppose $v_i \in M$ such that the projection of each v_i is v'_i, and let N be the submodule spanned by the v_i. Further, let $(0, 0, \dots a)$ generate the set of all $r \in R$ such that $(0, 0, \dots r) \in M$; such an a exists because the set of all such r is an ideal of R. We claim that $M = N \oplus \langle (0, 0, \dots a) \rangle$. Indeed, for any $v \in M$, choose a $u \in N$ such that the first $n - 1$ entries of v and u match. Then $v - u$ has zeroes in the first $n - 1$ entries, so it is in $\langle (0, 0, \dots a) \rangle$. Also the intersection of these two submodules is clearly 0, so the sum is a direct sum. Therefore M has a basis of size at most $k + 1 \leq n$. □

14 Module Homomorphisms

Module homomorphisms work the same way as linear maps between vector spaces: they are R-linear maps between two R-modules. The set of all such maps between two R-modules is denoted by $\mathrm{Hom}_R(M, N)$, and set of all maps from M to itself is denoted by $\mathrm{End}_R(M)$

Theorem 57. *For any R-modules M, N, $\mathrm{Hom}_R(M, N)$ is an R-module.*

Proof. Standard proof: If f, g are linear maps, then so are $f + g$ and $r \cdot f$ for any $r \in R$. □

Theorem 58. *If R is a commutative ring, then for any R-module M, $\mathrm{End}_R(M)$ is an R-algebra.*

Proof. It is enough to find a ring homomorphism from R to $\mathrm{End}_R(M)$ whose image lies in the center. For any $r \in R$, consider the endomorphism ϕ_r of M which sends v to $r \cdot v$ for any $v \in M$. Now by definition of R-linear map, ϕ_r commutes wit every endomorphism of M. Hence consider the map sending r to ϕ_r. This can be easily seen to be a homomorphism, whose image is in the center of $\mathrm{End}_R(M)$, as required. □

The above map $r \to \phi_r$ may not be injective. Indeed, consider the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$, then the endomorphisms $\phi_2, \phi_4, \phi_6, \dots$ are all the same. The map may not even be surjective. Indeed, look at $\mathbb{Z} \times \mathbb{Z}$ as a module over $\mathbb{Z}$, with term-wise addition. Then the linear map $(a, b) \to (a + b, 0)$ is not of the forn ϕ_r for any $r \in \mathbb{Z}$. In the special case where R is a field, we can check that ϕ_r is just the map $r \cdot I$ where I is the identity map.

We look at a special case of $\mathrm{End}_R(R)$. We claim that

$$\mathrm{End}_R(R) \cong R$$

as an R-algebra. Indeed, consider the map that sends ϕ to $\phi(1)$ for any endomorphism ϕ. We have $\phi(r) = r \cdot \phi(1)$ for all $r \in R$, so value of $\phi(1)$ completely determines ϕ. Also we have $(a\phi + b\psi)(1) = a\phi(1) + b\psi(1)$, and $(\phi \circ \psi)(1) = \psi(1) \cdot \phi(1)$, thus this map is indeed an injective homomorphism. To show that it is surjective, for any $r \in R$, look at the endomorphism $\phi_r(a) = r \cdot a$. Clearly this endomorphism satisfies $\phi_r(1) = r$, and thus the map is surjective. Finally, we have $\phi(1) = 1$ for the identity map ϕ, and so the construcetd map is indeed an isomorphism. In a similar way, we can actually prove

$$\mathrm{End}_R(R/I) \cong R/I$$

as R-algebras.

Note that $\mathbb{Z}_m$ is a $\mathbb{Z}$-module (we are using $\mathbb{Z}_m$ as a shorthand for $\mathbb{Z}/m\mathbb{Z}$). We will study $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$. Suppose ϕ is a homomorphism, and $\phi(1) = a$. Then for any $b \in \mathbb{Z}_m$, we have $\phi(b) = b \cdot \phi(1) = ab$. Thus $\phi(1)$ uniquely determines ϕ. However, when $b = m$, we must have

$$0 = \phi(0) = \phi(m) = m \cdot \phi(1) = ma$$

Thus we must have $n \mid ma$. This is possible only if $\frac{n}{\gcd(m,n)} \mid a$. Conversely, assume that we have such an a, and look at the map $b \to ab \pmod{n}$ from $\mathbb{Z}_m$ to $\mathbb{Z}_n$. This is clearly well-defined because $b \equiv b' \pmod{m} \implies m \mid b - b' \implies ma \mid ab - ab' \implies n \mid ab - ab'$. Also this map is clearly a linear map. Thus all possible values of $\phi(1)$ are elements of $\mathbb{Z}_n$ divisible by $\frac{n}{\gcd(m,n)}$. The set of these values is clearly a subring of $\mathbb{Z}_n$, and is in fact isomorphic to $\mathbb{Z}_{\gcd(m,n)}$ via the map $a \to \frac{a \cdot \gcd(m,n)}{n}$. Thus, doing the same thing as the above paragraph, we get

$$\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{\gcd(m,n)}$$

as $\mathbb{Z}$-modules. As a special case, if m, n are coprime, then $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \cong 0$. Also in the case of $\mathrm{End}(\mathbb{Z}_m)$, again by the same process as the above paragraph we get

$$\mathrm{End}(\mathbb{Z}_m) \cong \mathbb{Z}_m$$

as $\mathbb{Z}$-algebras.

We can also look at $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z})$ and $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_n)$. Again $\phi(1)$ uniquely determines the homomorphism. However, in the first case, if $\phi(1) = a \neq 0$, then we have

$$ma = m \cdot \phi(1) = \phi(m) = \phi(0) = 0$$

which is impossible. Hence we must have $\phi(1) = 0$, and so

$$\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}) \cong 0$$

In the second case, $\phi(1) = a \in \mathbb{Z}_n$ uniquely determines ϕ for any choice of a. Indeed, ϕ just becomes the map $b \to ab \pmod{n}$, which is a homomorphism. Therefore

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_n) \cong \mathbb{Z}_n$$

Theorem 59. *Let R be a ring, let I be an ideal of R, and let M, N be R/I-modules. Then, considering M, N as R-modules in the standard way, $\mathrm{Hom}_R(M, N)$ is an R/I-module, and*

$$\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{R/I}(M, N)$$

as R/I-modules.

Proof. The way we think of M, N as R-modules is the following: $r \cdot x = (r + I) \cdot x$. Now, for any R-linear map ϕ, we have $I\phi(x) = \phi(Ix) = \phi(0) = 0$, and so I annihilates $\mathrm{Hom}_R(M, N)$, and so it is an R/I-module. Next, for any R-linear map ϕ, we show that it is an R/I-linear map: indeed, we have $IM = IN = 0$, and so

$$(r + I) \cdot \phi(x) = \phi((r + I) \cdot x) = \phi(r \cdot x) = r \cdot \phi(x)$$

Conversely, any R/I-linear map can be lifted to an R-linear map as shown above. Hence the two homomorphism modules are isomorphic. □

For any R-module M and ideal I, consider $\mathrm{Hom}_R(R/I, M)$. Suppose ϕ is a homomorphism, and $\phi(1) = a$. Then for any $r \in I$, we have

$$ra = r \cdot \phi(1) = \phi(r) = \phi(0) = 0$$

Therefore $Ia = 0$. Also note that a uniquely determines ϕ. Therefore the set of values of a is just the submodule of M that is annihilated by I. In the similar way as the above proofs, we can show that $\mathrm{Hom}_R(R/I, M)$ is in fact isomorphic to this submodule. In particular, if no element of M is annihilated by I, then the homomorphism module is 0.

We can use this to ask about $\mathrm{Hom}_R(R/I, R/J)$, where I, J are ideals of R. This is isomorphic to the set of all $r \in R/J$ such that $sr = 0$ for all $s \in I$. This is equivalent to saying $Ir \in J$. If R is commutative, then this is clearly $[J : I]$. Therefore

$$\mathrm{Hom}_R(R/I, R/J) \cong [J : I]/J$$

In the case R is a PID, suppose $I = \langle a \rangle$ and $J = \langle b \rangle$. Then $Ir \in J$ iff $ar \in J$ iff $b \mid ar$. Since we are working in a PID, we can consider $d = \gcd(a, b)$. Then $\frac{a}{d}, \frac{b}{d}$ are coprime, and so we must have $\frac{b}{d} \mid r$. Now we proceed in the same way as the case for $\mathbb{Z}$, and we get

$$\mathrm{Hom}_R(R/\langle a \rangle, R/\langle b \rangle) \cong R/\langle \gcd(a, b) \rangle$$

The same idea will not work if we don't assume domain, because then there is no concept of division. We can still define $d = \langle a, b \rangle$, and if $a = a'd$ and $b = b'd$, we get that there is an $s \in R$ such that $a'rd = b'sd \iff a'r - b's$ is an annihilator of $d \iff a'r - b's$ is an annihilator of both a, b. If J_d is the ideal of annihilators of d, then we must have $a'r = b's$ in R/J_d. Now, a', b' are coprime in R/J_d, so we must have $b' \mid r \implies$ the set of all such r is $\langle b' \rangle$ in R/J_d, which lifts to $\langle b', d' \rangle$ in R, where d' is the generator of J_d. Now note that $dr \in \langle b \rangle$ iff $r \in \langle b', d' \rangle$. Therefore we get

$$\mathrm{Hom}_R(R/\langle a \rangle, R/\langle b \rangle) \cong \langle b', d' \rangle / \langle b \rangle$$

I couldn't go further than this.

We can say in general when $\mathrm{Hom}_R(M, N) = 0$:

Theorem 60. *Let M, N be R-modules. Then,* $\mathrm{Ann}(M) + \mathrm{Ann}(N) \subset \mathrm{Ann}(\mathrm{Hom}_R(M, N))$.

Proof. Suppose I, J are annihilators of M, N respectively. For any homomorphism ϕ, and any $a \in I$ and $b \in J$, we have

$$\phi(bx) = b \cdot \phi(x) = 0$$
$$\phi(ax) = \phi(0) = 0$$
$$\implies \phi((a + b)x) = (a + b)\phi(x) = 0$$

Hence $a + b$ annihilates $\mathrm{Hom}_R(M, N)$, which directly gives the result. □

15 Noetherian and Artinian Modules

Definition. An R-module M is called Noetherian if every submodule of M is finitely generated.

We have proved that if R is left-Noetherian, and M is finitely generated, then M is Noetherian. Similar to Noetherian rings, we have the following equivalence:

Theorem 61. *A module M is Noetherian iff for every increasing sequence of submodules $N_1 \subset N_2 \subset \cdots$, there is a positive integer m such that $N_{n+1} = N_n$ for all $n \geq m$.*

Proof. Assume M is Noetherian, then if $N_1 \subset N_2 \subset \cdots$ is an increasing sequence of submodules, then the union of all N_i, say N, is a submodule of M. Hence it can be generated by finitely many elements $x_1, x_2, \dots x_k$. But there must be some m such that all the x_i are in N_m, and so $N_m = N_{m+1} = N_{m+2} = \cdots = N$, as required.

Conversely, if N is a submodule that cannot be finitely generated, then we can choose an infinite sequence of elements $x_i \in N$ such that $x_{i+1} \notin \langle x_1, \dots x_i \rangle$ for each i. Then we get the strictly increasing sequence of submodules: $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots$ □

In a similar way, we can define Artinian modules.

Definition. A module M is called Artinian if for every decreasing sequence of submodules $N_1 \supset N_2 \supset \cdots$, there is a positive integer m such that $N_{n+1} = N_n$ for all $n \geq m$.

Definition. A short exact sequence is a sequence of R-modules L, M, N, as well as homomorphisms $\psi : L \to M$ and $\phi : M \to N$ such that ψ is injective, ϕ is surjective, and $\ker(\phi) = \mathrm{Im}(\psi)$. A short exact sequence is denoted by

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\phi} N \to 0$$

(sometimes without the 0s at the ends)

Basically, L can be embedded in M, and we have $N \cong M/L$ in some sense.

In a short exact sequence, clearly if L, N are finitely generated, then M is also finitely generated; in fact it is generated by the union of sets of generators of L and N.

Theorem 62. *In a short exact sequence $0 \to L \xrightarrow{\psi} M \xrightarrow{\phi} N \to 0$, L, N are Noetherian iff M in Noetherian.*

Proof. If M is Noetherian, then so are L, N: Because every submodule of N is a quotient of a submodule of M, and every submodule of L is a submodule of M. Now we prove the converse.

Let $I_1 \subset I_2 \subset \cdots$ be an increasing sequence of submodules of M. Then $I_1 \cap L \subset I_2 \cap L \subset \cdots$ and $(I_1 + L)/L \subset (I_2 + L)/L \subset \cdots$ are increasing sequences of submodules of L, N respectively. Therefore both of them are eventually constant. Choose a large n, and suppose there is an $x \in I_{n+1}$ that is not in I_n. From the second sequence being constant, there must be a $y \in L$ such that $x + y \in I_n \subset I_{n+1}$. Hence $y \in I_{n+1} \cap L = I_n \cap L$, and hence we get $x \in I_n$, contradiction! Hence the sequence is eventually constant, and so M is Noetherian. □

Note that the above proof only using the ascending chain condition for Noetherian modules. Therefore if we just flip the ascending chains to descending chains in the above proof, we can prove the following:

Theorem 63. *In a short exact sequence $0 \to L \xrightarrow{\psi} M \xrightarrow{\phi} N \to 0$, L, N are Artinian iff M in Artinian.*

Note that any direct sum of modules can be thought of as a short exact sequence: If $M = L \oplus N$, then $L \xrightarrow{\psi} M \xrightarrow{\phi} N$. ψ can be the natural map $a \to a + 0$, and ϕ can be thought of as the map $a + b \to b$ for any $a \in L, b \in N$. Therefore using the above theorem, we get that if R is left-Noetherian, then the module R^n is Noetherian for any positive integer n. We also have the following result, which gives another proof that every finitely generated R-module is Noetherian if R is left-Noetherian:

Theorem 64. *Let M be an R-module that is generated by a set of n generators, $n \in \mathbb{N}$. Then there is a submodule $N \subset R^n$ such that $M \cong R^n/N$.*

Proof. Let $x_1, x_2, \dots x_n$ be the generators of M, and consider the linear map $R^n \to M$ given by $(a_1, a_2, \dots a_n) \to a_1x_1 + a_2x_2 + \cdots a_nx_n$. Clearly this is surjective, and if N is the kernel of this map, we get the result by the first isomorphism theorem. □

Note that the above result also proves the following:

Theorem 65. *Let R be an Artinian ring, and let M be a finitely generated R-module. Then M is Artinian.*

We note that if M is a finitely generated free module, say with a basis having n elements, then $M \cong R^n$. A question we can ask is this: Do two sets of basis elements of a finitely generated free module have the same size? This is true if we assume the original module is Noetherian:

Theorem 66. *Let M be a Noetherian free module. Then any two sets of basis elements of M have the same size.*

Proof. It is sufficient to prove that if R^m is Noetherian, then R^m and R^n are not isomorphic if $n < m$. We will in fact show that any $n+1$ elements of R^n are linearly dependent. FTSOC we have $n+1$ linearly independent elements $x_{1,1}, x_{1,2}, \ldots x_{1,n}, y_1$. Then note that $\langle x_{1,1}, x_{1,2}, \ldots x_{1,n} \rangle \cong R^n$, so it contains $n+1$ linearly independent elements $x_{2,1}, x_{2,2}, \ldots x_{2,n}, y_2$. In this way we can construct an infinite sequence of elements $y_1, y_2, \ldots$ and an infinite sequence of submodules

$$\langle y_1 \rangle \subset \langle y_1, y_2 \rangle \subset \langle y_1, y_2, y_3 \rangle \subset \cdots$$

Each inclusion is strict, because $\langle y_1, y_2, \ldots y_k \rangle$ doesn't interset $\langle x_{k,1}, x_{k,2}, \ldots x_{k,n}$, while $\langle y_1, y_2, \ldots y_{k+1} \rangle$ does. However this contradicts the assumption that M is Noetherian! □

In particular, if R is left-Noetherian, than any R-module has this property. However, this property always holds if R is commutative:

Theorem 67. *Let R be a commutative ring, and let M be a finitely generated free R-module. Then any two sets of basis elements of M have the same size.*

Proof. Assume that some R-module M has two sets of bases $x_1, \ldots x_n$ and $y_1, \ldots y_m$. Write

$$y_i = \sum_{j=1}^{n} a_{i,j} x_j$$

$$x_j = \sum_{i=1}^{m} b_{i,j} y_i$$

For some coefficients in R. Putting the expressions for all the x_j in the expression for y_k for some k and comparing the coefficient of y_k gives

$$1 = \sum_{j=1}^{n} a_{k,j} b_{k,j}$$

Summing over all $k \leq m$, we get

$$m = \sum_{k=1}^{m} \sum_{j=1}^{n} a_{k,j} b_{k,j}$$

Now, in the similar way, we can put the expressions for all the y_k in the expression for x_j for some j and compare the coefficient of x_j, to get

$$1 = \sum_{k=1}^{n} b_{k,j} a_{k,j}$$

Summing over all $j \leq n$, we get

$$n = \sum_{j=1}^{n} \sum_{k=1}^{m} b_{k,j} a_{k,j}$$

However, since R is commutative, these two sums must be equal, so we get $m = n$ as required.

A more succinct way to write the proof is the following: Let A be the $m \times n$ matrix that transforms the x_j into the y_i, and let B be the $n \times m$ matrix that transforms the y_i into the x_j. Then by substituting the two sets of expressions into each other and comparing coefficients, we get

$$AB = I_m \text{ and } BA = I_n$$

where I_m, I_n are the identity matrices. However, by the algebraic fact that trace(AB) = trace(BA) for any matrices A, B (whenever the product is commutative), we directly get $m = n$. □

There is another proof of the above theorem, but for that we need the following:

Theorem 68. *Let R be a commutative ring, and let F be a free R-module having a basis with cardinality κ. Then, for any proper ideal I and multiplicatively closed subset A of R,*

1. *F/IF is a free module over R/I having a basis with cardinality κ.*
2. *$A^{-1}F$ is a free module over $A^{-1}R$ having a basis with cardinality κ.*

Proof. For the first part, note that F/IF is a module over R/I because $I(F/IF) = 0$. Let B be a basis of F over R with $|B| = \kappa$. Clearly $B + IF$ generates F/IF over R/I, and has cardinality at most κ. Also, $B + IF$ is linearly independent over R/I, because if some $\sum(a_j + I)(x_j + IF) = 0$, then $\sum a_j x_j \in IF \implies a_j \in I$ because B is a basis of F. This also proves that cardinality of $B + IF$ is exactly κ, because $x_i + IF = x_j + IF \implies x_i = x_j$ in R/I, which implies $i = j$ due to linear independence because $1 \notin I$.

A similar thing can be done for $A^{-1}F$, by taking $\frac{B}{1}$. Indeed, this spans $A^{-1}F$, and is linearly independent because $\sum \frac{a_j x_j}{r_j} = 0 \implies$ there is some $s \in A$ such that $a_j r_1 \cdots r_{j-1} r_{j+1} \cdots r_m s = 0$ for each j (by direct expansion). Therefore each a_j is annihilated by some element of A, and so each $\frac{a_j}{r_j} = 0$, as required. This also proves that $|\frac{B}{1}| = \kappa$. □

Now, suppose R is a commutative ring, and let F be a free module. Assume FTSOC that there are two bases of F having cardinalities $\kappa < \mu$. Choose I to be a maximal ideal of R. Then F/IF is a vector space over the field R/I, but it has two different bases of cardinalities κ and μ, which is a contradiction.

In the case R is an integral domain, we can instead choose A to be the set of non-zero elements of R. Then $A^{-1}R$ is the field of fractions K of R, and $A^{-1}F$ is a vector space over K, so all of its bases have the same cardinality.

One question to ask: Is every Artinian module Noetherian? If R is a field, then it is easy to see that a module is Artinian iff it is a finite dimensional vector space iff it is Noetherian. However, this is not true in general.

Let $\mathbb{Z}_{(p)}$ denote $\mathbb{Z}$ localized outside the prime ideal $\langle p \rangle$. Consider the $\mathbb{Z}_{(p)}$-module $\mathbb{Q}/\mathbb{Z}_{(p)}$. This is not Noetherian, because for any finite set $\{r_1, r_2, \ldots r_n\}$, if we take a prime power p^m larger than the denominators of all the r_i, then $\frac{1}{p^m}$ cannot be generated. But, it is Artinian because of the following theorem:

Theorem 69. *Let R be a PID with finitely many maximal ideals, and let K be the field of fractions of R. Then K/R is an Artinian R-module.*

Proof. Let $p_1, p_2, \ldots p_k$ be the maximal primes of R. Then note that we can write any element of K as $\frac{a}{s}$ for some coprime $a, s \in R$ and such that all prime factors of s are from the p_i (as any element not divisible by any p_i is invertible in R). Now for any submodule $N \subset K/R$, we claim that $\frac{a}{s} \in N$ when $\gcd(a, s) = 1 \implies \frac{1}{s} \in N$. Indeed, by Bezout's lemma there is a b such that $ab \equiv 1 \pmod{s}$, and so $b \cdot \frac{a}{s} = \frac{1}{s}$ in N, which proves the claim.

Thus any submodule is uniquely determined by the set of denominators of the reduced fractions that occur in it. For any $i \leq k$ and submodule N, let $v_i(N)$ denote the largest power of p_i that divides one of these reduced denominators, and let $v_i(N) = \omega$ if no largest power exists. Note that the reduced denominator of $\frac{1}{s} + \frac{1}{r}$ is $\mathrm{lcm}(r, s)$, so in fact the k values of $v_i(N)$ uniquely determine a submodule (because we can just bunch up the largest powers together). Further, if $N_1 \supset N_2$, then $v_i(N_2) \leq v_i(N_1)$, with equality for all i iff the submodules are equal.

Now assume there is a descending chain $N_1 \supset N_2 \supset \cdots$ of submodules. For each i, $v_i(N_j)$ is a decreasing sequence, and it cannot keep decreasing forever (because it is a well-order with order type ω). Thus for all large j, $v_i(N_j)$ is constant. Since there are only finitely many i, after one point all of the $v_i(N_j)$ will be constant, and so N_j will be eventually constant, as required. □

The theorem doesn't hold if we allow infinitely many maximal ideals. Just consider the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$. We construct a strictly decreasing chain $N_1 \supset N_2 \supset \cdots$ as follows: N_i is the set of all fractions in $\mathbb{Q}/\mathbb{Z}$ with denominators (in their reduced form) not divisible by any of the first i primes.

16 Bootstrapping

We only look at commutative rings in this section.

Suppose $(R, \mathfrak{m})$ is a local ring, such that $\mathfrak{m}^n = 0$ for some n. Look at the series

$$R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots \supset \mathfrak{m}^{n-1} \supset \mathfrak{m}^n = 0$$

Each successive quotient in this series is a vector space over the field $k = R/\mathfrak{m}$. This vector space has a finite dimension if $\mathfrak{m}$ is finitely generated. Further, the sequence $0 \to \mathfrak{m}^l \to \mathfrak{m}^{l-1} \to \mathfrak{m}^{l-1}/\mathfrak{m}^l \to 0$ is a short exact sequence of R-modules; $0 \to \mathfrak{m} \to R \to R/\mathfrak{m}$ is also a short exact sequence. Using properties of short exact sequences, and the fact that the series ends at a 0, we can piece together information about R itself. This is called bootstrapping.

Theorem 70. *Suppose $(R, \mathfrak{m})$ is a local ring, such that $\mathfrak{m}$ is finitely generated and $\mathfrak{m}^n = 0$ for some n. Then R is Artinian.*

Proof. We prove that, for any l, $\mathfrak{m}^l$ is an Artinian R-module. We denote R by $\mathfrak{m}^0$. We use backwards induction on l, starting with $l = n$: $\mathfrak{m}^l = 0$, which is Artinian. Now assume it is true for some $l \leq n$. Since $\mathfrak{m}^{l-1}/\mathfrak{m}^l$ is a finite dimensional $R/\mathfrak{m}$-vector space, and any submodule of it is also a vector subspace, it must be Artinian. Now we know that the endpoints of the short exact sequence $\mathfrak{m}^l \to \mathfrak{m}^{l-1} \to \mathfrak{m}^{l-1}/\mathfrak{m}^l$ are Artinian, and hence the middle term is also Artinian. Therefore we are done by induction. □

Note that if $\mathfrak{m}_1, \mathfrak{m}_2, \ldots \mathfrak{m}_k$ are maximal ideals, then we also have a series of short exact sequences $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_l \to \mathfrak{m}_1 \cdots \mathfrak{m}_{l-1} \to \mathfrak{m}_1 \cdots \mathfrak{m}_{l-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_l$, and the right term is again a vector space over the field $R/\mathfrak{m}_l$ (again the empty product is R). Thus we don't need all the $\mathfrak{m}_i$ to be the same; we can still do bootstrapping. Thus we can generalize the above result:

Theorem 71. *Let R be a ring, such that some finite product of maximal ideals of R is 0. Then R is Artinian.*

Theorem 72. *Let R be a Noetherian ring having finitely many prime ideals, all of which are maximal. Then R is Artinian.*

Proof. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots \mathfrak{m}_k$ be all the prime ideals of R. From the above theorem, it is sufficient to prove that $(\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_k)^n = 0$ for some n. However, since all the $\mathfrak{m}_i$ are comaximal, and the nilradical $\mathrm{Nil}(R)$ of R is the intersection of all the $\mathfrak{m}_i$, $\mathfrak{m}_1 \cdots \mathfrak{m}_k = \mathrm{Nil}(R)$. Since R is Noetherian, $\mathrm{Nil}(R)$ is finitely generated, say by $r_1, r_2, \ldots r_m$, such that $r_i^{n_i} = 0$. Therefore, for large $n > n_1 + n_2 + \cdots + n_m$, we must have $\mathrm{Nil}(R)^n = 0$, as required. □

However, we don't even need the condition that there are only finitely many prime ideals. Indeed, since every prime ideal is maximal, every prime ideal is also minimal, and since any Noetherian ring has only finitely many minimal prime ideals, we get the required statement.

In fact, we can get a complete characterization of Artinian rings. For this we use the following lemma:

Theorem 73. *The Jacobson radical of any Artinian ring is nilpotent.*

Proof. Since all primes are maximal in any Artinian ring, the Jacobson radical is the nilradical. Let J be the Jacobson radical of an Artinian ring R. Note that $J \supset J^2 \supset \cdots$ is a decreasing sequence of ideals, and so must stabilize at some point. Say $J^n = J^{n+1}$. We prove that $J^n = 0$. Assume the contrary. Let I be a minimal non-zero ideal satisfying $JI = I$. Such an ideal exists because the set of all non-zero ideals satisfying $JI = I$ is non-empty (since J^n is in it), and any non-empty set of ideals has a minimal element in an Artinian ring by Zorn's lemma.

In order to give a contradiction, we show that $I = 0$ by showing $JI = 0$. We do this by showing that $xI = 0$ for any $x \in J$. For any $x \in J$, $J \cdot (xI) = xI$ as well, so either $xI = 0$ or $xI = I$. If $x \in J$, then $xI = I \implies I = xI = x^2I = \cdots x^mI = 0$ for some m, since every element in J is nilpotent. Therefore $xI = 0$ for all $x \in J \implies JI = 0 \implies I = JI = 0$, again a contradiction! Therefore $J^n = 0$, as required. □

Theorem 74. *Let R be a commutative ring. The following are equivalent:*

1. *R is Artinian.*

2. *R is Noetherian and all of its prime ideals are maximal.*

Proof. We have already proved $(2) \implies (1)$. Now assume R is Artinian. We have already proved that all prime ideals of R are maximal, and that there are finitely many maximal ideals. Further, we have proved that the Jacobson radical is nilpotent, so some finite product of maximal ideals is 0. Suppose $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_k = 0$ where each $\mathfrak{m}_i$ is a maximal ideal of R. Consider the short exact sequence

$$0 \to \mathfrak{m}_1\cdots\mathfrak{m}_l \to \mathfrak{m}_1\cdots\mathfrak{m}_{l-1} \to \mathfrak{m}_1\cdots\mathfrak{m}_{l-1}/\mathfrak{m}_1\cdots\mathfrak{m}_l \to 0$$

Again the empty product stands for R. The right hand term is always Noetherian. This is because it is an Artinian R-module which is annihilated by $\mathfrak{m}_l$, and hence is an Artinian vector space over the field $R/\mathfrak{m}_l$. However, a vector space is Artinian iff it is finite dimensional iff it is Noetherian, so the right hand term is Noetherian.

We will use backwards induction on l to prove that $\mathfrak{m}_1\cdots\mathfrak{m}_l$ is Noetherian. Base case: $l = k$, the product is 0, which is Noetherian. Now assume the product is Noetherian from some l. Hence the left hand term of the above short exact sequence is also Noetherian, and so we can deduce that the middle term, i.e., $\mathfrak{m}_1\cdots\mathfrak{m}_{l-1}$ is also Noetherian. Hence we are done by induction, and so R is Noetherian. □

We can actually generalise the above result, in two ways:

Theorem 75. *Let R be an Artinian ring. Then any Artinian R-module is Noetherian.*

Proof. The proof is very similar to the above proof. As before, some product $\mathfrak{m}_1\cdots\mathfrak{m}_k$ of maximal ideals in R is 0. This time, we look at short exact sequences of the form

$$0 \to \mathfrak{m}_1\cdots\mathfrak{m}_lM \to \mathfrak{m}_1\cdots\mathfrak{m}_{l-1}M \to \mathfrak{m}_1\cdots\mathfrak{m}_{l-1}M/\mathfrak{m}_1\cdots\mathfrak{m}_lM \to 0$$

where M is the given Artinian module. As before, the RHS is always an Noetherian R-module since it is an Artinian $R/\mathfrak{m}_l$-vector space, and again by backwards induction we can show that $\mathfrak{m}_1\cdots\mathfrak{m}_lM$ is Noetherian for all l, which proves that M is Noetherian. □

Theorem 76. *Any finitely generated Artinian module is Noetherian.*

Proof. Let M be a finitely generated Artinian R-module. Let $I = \text{Ann}_R(M)$. Then M is an R/I-module, with annihilatro being 0. We claim that R/I is an Artinian ring. Indeed, let $J_1 \supset J_2 \supset \cdots$ be a descending chain of ideals in R/I. For any $x \in M$, $J_1x \supset J_2x \supset \cdots$ is a decreasing sequence of submodules of M, so it must stabilize at some point, i.e., $J_nx = J_{n+1}x$ for all n greater than some $N(x)$, for every $x \in M$. Assume M is generated by $x_1, x_2, \ldots x_m$, and choose some $N > N(x_1), N(x_2), \ldots N(x_m)$. Thus $J_{n+1}x = J_nx$ for all $x \in M$ and all $n > N$. This means that $J_{n+1} = J_n$, since annihilator of M is 0. Therefore the sequence stabilizes, and R/I is Artinian, as required.

Now by the above theorem, any Artinian module over an Artinian ring (R/I in this case) is Noetherian, and so we are done. □

The proof of the above theorem in fact gives something stronger:

Theorem 77. *Let M be a finitely generated Artinian (resp. Noetherian) R-module. Then $R/\text{Ann}_R(M)$ is an Artinian (resp. Noetherian) ring.*

17 Idempotents in Rings

We only consider commutative rings in this section.

Definition. An element $e \in R$ is called idempotent is $e^2 = e$.

Clearly $0, 1$ are idempotent elements in any ring. We can ask, when will there be any non-trivial idempotents?

Theorem 78. *A ring R contains non-trivial idempotents iff $R \cong S_1 \times S_2$ for some (non-zero) rings S_1, S_2 .*

Proof. Assume that $R \cong S_1 \times S_2$. Then the element corresponding to $(1, 0)$ is a non-trivial idempotent of R. Conversely, assume R has a non-trivial idempotent e. Let $I = \langle e \rangle$ and $J = \langle 1 - e \rangle$. Note that $I + J = R$ since $e + (1 - e) = 1$, and $IJ = 0$ because $e(1 - e) = 0$. Further, neither e nor $1 - e$ is a unit; otherwise, from $e(1 - e) = 0$ we get $e = 0$ or $e = 1$. Therefore the rings $S_1 = R/I$ and $S_2 = R/J$ are non-zero rings. Then by CRT, we have

$$R \cong R/IJ \cong S_1 \times S_2$$

as required. □

In fact we can characterize rings with finitely many idempotents.

Theorem 79. *Let R be a ring such that there exists a largest positive integer n for which we can write $R = S_1 \times S_2 \times \cdots \times S_n$ for some non-zero rings S_i. Then R contains exactly 2^n idempotents.*

Proof. We know that each S_i cannot be further decomposed into a product of rings. Hence each S_i only contains trivial idempotents. Further, each idempotent of R has the form $(e_1, e_2, \ldots e_n)$ for some idempotents $e_i \in S_i$. Thus the result follows. □

As a corollary, we have:

Theorem 80. *Let R be a ring with finitely many maximal ideals, say n of them. Then R has at most 2^n idempotents.*

In particular, local rings have no non-trivial idempotents.

18 Decomposition of Modules

Again we only consider commutative rings.

Definition. A module M is called decomposable if there exist non-zero submodules N_1, N_2 such that $M \equiv N_1 \oplus N_2$. M is called indecomposable otherwise.

Theorem 81. *A ring is decomposable as a module over itself iff it can be written as a product of two non-zero rings.*

Proof. Assume $R \equiv S_1 \times S_2$. Then $I = S_1 \times \{0\}$ and $J = \{0\} \times S_2$ are ideals of R, such that $I + J = R$ and $I \cap J = (0, 0) = 0$. Further, they are non-zero because S_1, S_2 are non-zero. Hence $R = I \oplus J$ is decomposable.

Conversely, assume $R = I \oplus J$ for some non-zero ideals $I, J \subset R$. Then none of I, J are equal to R, because then the other must be 0. Therefore by CRT

$$R \cong R/(I \cap J) \cong S_1 \times S_2$$

where $S_1 = R/I$ and $S_2 = R/J$ are both non-zero. □

Theorem 82. *An R-module M is indecomposable iff the ring $\mathrm{End}_R(M)$ contains no non-trivial idempotent elements.*

Proof. Assume $M = N_1 \oplus N_2$. Then the projection map $(x, y) \to (x, 0)$ is a non-trivial idempotent of $\mathrm{End}_R(M)$.

Now assume $f^2 = f \in \mathrm{End}_R(M)$ where $f \neq 0, \mathrm{Id}$. Let $N_1 = fM$ and $N_2 = (1 - f)M$ (here 1 stands for identity). Clearly $N_1 + N_2 = M$ because $f(x) + (1 - f)(x) = x$. Also, $z \in N_1 \cap N_2 \implies z = f(x) = y - f(y)$ for some $x, y \in M \implies f(x) = f(f(x)) = f(y - f(y)) = 0 \implies z = 0$, so $N_1 \cap N_2 = \{0\}$, and so $M = N_1 \oplus N_2$, as required. □

We can also say something about simple modules using the endomorphism ring.

Theorem 83. *An R-module M is simple iff $\mathrm{End}_R(M)$ is a skew field.*

Proof. First note that any simple module can be generated by any non-zero element of that module. Indeed, if $x \neq 0$ is in M, then we must have $\langle x \rangle = M$ since M is simple. Therefore, if we fix any $x_0 \in M$, any endomprphism f is uniquely determined by $f(x_0)$; conversely, given $f(x_0)$, we can construct the required endomorphism. The endomorphism is non-zero iff $f(x_0) \neq 0$. This holds for any $x_0 \in M$. This immediately proves that $\mathrm{End}_R(M)$ is a skew field: for any non-zero endomorphism f, assume $f(x_0) = y_0 \neq 0$. Then look at the endomorphism g that sends y_0 to x_0: this is the inverse of f.

Conversely, assume $\mathrm{End}_R(M)$ is a skew field. This means that any non-zero endomorphism is bijective: $f \circ g = g \circ f = \mathrm{Id}$ implies f is bijective. □

Definition. Let M be an R-module. A submodule $N \subset M$ is called reducible if it can be written as an intersection of two subomdules that properly contain N. Else it is called irreducible.

Theorem 84. *Let M be a Noetherian module. Then any submodule of M can be written as a finite intersection of irreducible submodules.*

Proof. Assume the contrary, and consider the non-empty collection of all submodules that cannot be written as a finite intersection of irreducible submodules. Since M is Noetherian, this collection has a maximal element; call it N. Then N must be reducible, so write $N = N_1 \cap N_2$ for some $N \subsetneq N_1, N_2$. Then each of N_1, N_2 can be written as a finite intersection of irreducible submodules, so N can also be written as thus, contradiction! □

Theorem 85. *Any Noetherian or Artinian module can be written as a finite direct sum of indecomposable modules.*

Proof. Let M be a Noetherian module, and assume FTSOC that it cannot be written as a finite sum of indecomposables. Then M is decomposable, so write it as $M = M_1 \oplus N_1$, where $M_1, N_1 \neq 0$. Now one of M_1, N_1 is decomposable: say N_1. Again write $N_1 = M_2 \oplus N_2$ where N_2 is decomposable, and so on. Thus we get a strictly increasing sequence of submodules

$$M_1 \subset M_1 \oplus M_2 \subset M_1 \oplus M_2 \oplus M_3 \subset \cdots$$

which contradicts Noetherian-ness. If the module is Artinian, □

19 Composition Series

Definition. A composition series of a module M is an increasing series of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$$

such that each successive quotient M_{i+1}/M_i is a simple module.

Theorem 86. *A module has a composition series iff it is both Artinian and Noetherian.*

Proof. Let M be a Noetherian and Artinian R-module. Passing over to $R/\mathrm{Ann}_R(M)$ if necessary, we can assume R is Artinian. Then M has a prime filtration $M_0 \subset M_1 \subset \cdots \subset M_n$. Here $M_{i+1}/M_i = R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$. We claim that each $\mathfrak{p}_i$ is maximal. Indeed, M_{i+1}/M_i is an Artinian module, so as a ring $R/\mathfrak{p}$ is Artinian, which is only possible if $\mathfrak{p}$ is maximal. Therefore each successive quotient is a simple module.

Conversely, suppose M has a simple filtration. Consider each short exact sequence $0 \to M_i \to M_{i+1} \to M_{i+1}/M_i \to 0$. Since every simple module is both Noetherian and Artinian, then by bootstrapping we can prove each M_i is both Artinian and Noetherian, which proves the result for M_n. □

Definition. A Noetherian and Artinian module is called a module of finite length.

Theorem 87. *Let M be a module of finite length. Then any two simple filtrations of M have the same size.*

Proof. Assume the contrary. Call a module of finite length "bad" if there exist two simple filtrations of it with different lengths. Consider the collection of bad submodules of M. This has a minimal element, say N. Note that N is neither zero nor simple. Let $N_0, N_1, \ldots N_n$ and $N'_0, N'_1, \ldots N'_m$ be two simple filtrations of different lengths, say $2 \leq n < m$. Then $L = N'_{m-1}$ only has simple filtrations of length $m-1$, by minimality of N. However consider the sequence $0 = N_0 \cap L \subset N_1 \cap L \subset \cdots \subset N_n \cap L = L$. We claim that every successive quotient is either 0 or simple. Indeed, if $N_{i+1} \cap L$ and $N_i \cap L$ have a proper non-zero submodule L' in between, then $N_i + L'$ is a submodule strictly between N_i and N_{i+1}, contradiction! Thus we get an increasing sequence of submodules, which gives a simple filtration of size at most $n \leq m-1$. Thus equality holds, and each inclusion in the above series is strict.

Now we claim that $N_i \subset L$ for each i, and we prove this by induction. Clearly this is true for $i = 0$, so assume it is true for some $i \geq 0$. If N_{i+1} is not a subset of L, then $N_i \subsetneq N_{i+1} \cap L \subsetneq N_{i+1}$ is a module strictly between N_i and N_{i+1}, contradiction! Thus $N_i \subset L$ for each i, and for $i = n$ we get $N \subset L$, which gives us our final contradiction! □

In particular, finitely generated modules over Artinian rings have finite length. However, if there is a field contained in the ring, we can say something about the length of any finitely generated module.

Theorem 88. *Let $(R, \mathfrak{m})$ be a local Artinian ring, such that there exists a field $k \cong R/\mathfrak{m}$ embedded as a subring of R. Let M be a finitely generated R-module. Then M is a finite dimensional k-vector space, and $\ell(M) = \dim_k(M)$.*

Proof. We prove this using induction on $\ell(M)$. In case M is simple, $M \cong R/\mathfrak{m} = k$ as R-modules, and hence also as $R/\mathfrak{m} = k$-vector spaces. This has dimension 1, as required.

Now assume the theorem is true when $\ell(M) < n$, for some $n \geq 2$. Take module N with length n, and let M be a maximal submodule of N. Then $0 \to M \to N \to M/N \to 0$ is a short exact sequence of R-modules, and hence also k-vector spaces. Since M/N is simple, again it is isomorphic to $R/\mathfrak{m} = k$ as a k-vector space. Hence using rank-nullity theorem, $\dim_k(N) = 1 + \dim_k(M) = 1 + \ell(M) = \ell(N)$, as required. □

Does any subfield k work for the above? No, for example $\mathbb{Q}$ is a subfield of $\mathbb{R}$, and length of any field is 1, but $\dim_{\mathbb{Q}}(\mathbb{R})$ is infinite.

Thus we require a specific kind of subfield. Note that for any subfield k, there is a map

$$k \subset R \to R/\mathfrak{m}$$

into $R/\mathfrak{m}$, so $R/\mathfrak{m}$ is a "maximal" subfield of R. Is this subfield always guaranteed to exist?

Theorem 89. *Let $(R, \mathfrak{m})$ be a local Artinian ring, such that some non-zero subfield is a subring of R. Then there exist a field $k \cong R/\mathfrak{m}$ embedded as a subring of R.*

Proof. Let k be a maximal subfield contained in R. Existence of such a subfield is guaranteed by Zorn's lemma. Assume $k \neq R/\mathfrak{m}$. Let a be a unit not in k. Then $k[a]$ is not a field, so there exists a polynomial $f \in k[x]$ such that $f(a)$ is not zero, and neither a unit, i.e., $f(a) \in \mathfrak{m} \setminus \{0\}$. We can also assume that f has minimum possible degree. Call f the "minimal polynomial" of a. By Euclidean algorithm in $R/\mathfrak{m}$, we get that if $g(a) \in \mathfrak{m}$, then $f \mid g$. In particular, the minimal polynomial is unique upto scaling. Choose an $a \notin k$ with minimum possible degree of its minimal polynomial.

Since R is Artinian, there exists an n such that $\mathfrak{m}^n = 0$. We will construct a sequence $a = a_1, a_2, \dots a_n$, all equivalent modulo $\mathfrak{m}$, such that f is the minimal polynomial of each a_i, and $f(a_i) \in \mathfrak{m}^i$ for each i. Indeed, assume we have constructed this sequence up to some a_i ($i = 1$ case was already given). Expanding modulo $\mathfrak{m}^{i+1}$, we get $f(a_i + t) \equiv f(a_i) + tf'(a_i) \pmod{\mathfrak{m}^{i+1}}$, for any $t \in \mathfrak{m}^i$. Since no minimal polynomial has degree less than $\deg f$, $f'(a_i)$ must be a unit. Hence in the above, we can take $t = -\frac{f(a_i)}{f'(a_i)} \in \mathfrak{m}^i$, and $a_{i+1} = a_i + t$ to get $f(a_{i+1}) \in \mathfrak{m}^{i+1}$. Since degree of minimal polynomial of a_{i+1} is at least $\deg f$, f must be the minimal polynomial of a_{i+1}, as required.

Therefore $f(a_n) \in \mathfrak{m}^n \implies f(a_n) = 0$. We claim that $k[a_n]$ is a field. Indeed, if for some $g \in k[x]$, if $g(a_n) \in \mathfrak{m}$, then $f \mid g \implies g(a_n) = 0$. Therefore $k[a_n]$ is a proper algebraic extension of k, which contradicts maximality of k. Therefore $k \cong R/\mathfrak{m}$. □

20 Zariski Topology

For any ideal I, let $V(I)$ denote the set of all prime ideals containing I.

Definition. The Zariski topology on a commutative ring R is the topology on $\operatorname{Spec}(R)$ with the closed sets being $V(I)$ for ideals $I \subset R$.

We can verify that this indeed forms a topology.

Theorem 90. $\operatorname{Spec}(R)$ *is compact.*

Proof. Let U_i, $i \in \Lambda$ be an open cover of $\operatorname{Spec}(R)$. Let V_i be complements of U_i, so each $V_i = V(I_i)$ for some ideal I_i such that intersection of all V_i is empty. It is sufficient to prove that intersection of some finite subset of the V_is is empty. Note that we have $\bigoplus_{i \in \Lambda} I_i = R$, since otherwise some maximal ideal $\mathfrak{m}$ contains the sum, and so $\mathfrak{m} \in V_i$ for each i, contradiction! Therefore there exist finitely many subsets $i_1, i_2, \dots i_k$ and elements $a_{i_j} \in I_i$ such that $1 = a_{i_1} + \cdots + a_{i_k}$, so $\bigoplus_{j=1}^{k} I_{i_j} = R$. Now if intersection of all V_{i_j} is not empty, then there is some prime $\mathfrak{p}$ containing each I_{i_j}, but then it will also containing its direct sum, contradiction! □

When is this topology connected?

Theorem 91. Spec(R) *is connected iff* R *has no non-trivial idempotents.*

Proof. First assume R has non-trivial idempotents. Then we know that there exist ideals non-zero proper ideals $I, J \in R$ such that $IJ = 0$ and $I + J = R$. Then $V(I)$ and $V(J)$ are disjoint, and since $IJ = 0$, every prime ideal is in either $V(I)$ or $V(J)$, and hence $V(I)$ is a proper non-empty open and closed set of Spec(R), and so Spec(R) is disconnected.

Conversely, assume Spec(R) is disconnected, say $V(I), V(J)$ is a partition of Spec(R) into disjoint non-empty proper closed sets. Then $I + J = R$, and $IJ \in \mathfrak{p}$ for all primes $\mathfrak{p} \implies IJ \in \text{Nil}(R)$. We claim that we can assume I, J are finitely generated. Indeed, for any $x \in I$, let U_x denote the complement of $V(\langle x \rangle)$. Then $\{U_x\}$ is an open cover of $V(J)$, since for any $\mathfrak{p} \in V(J)$, there is some $x \in I$ such that $x \notin \mathfrak{p} \implies \mathfrak{p} \in U_x$. Since Spec$(R)$ is compact and $V(J)$ is closed, $V(J)$ is also compact, so there is a finite subcover $U_{x_1}, U_{x_2}, \dots U_{x_k}$ of $V(J)$.

Let $I' = \langle x_1, \dots x_k \rangle \subset I$. Clearly $V(I) \subset V(I')$, and since

$$V(I')^c = U_{x_1} \cup \cdots \cup U_{x_k} \supset V(J) = V(I)^c$$

we must in fact have $V(I) = V(I')$. Thus I can be replaced by the finitely generated I', and similarly for J.

Now, we have IJ is finitely generated, and every element of IJ is nilpotent, so ther exists an $n > 0$ such that $(IJ)^n = I^n J^n = 0$. Further, $I + J = R \implies I^n + J^n = R$, so R must have non-trivial idempotents, as required. □

Theorem 92. *Let* $\phi : R \to S$ *be a ring homomorphism. Then the lifting map* $\psi :$ Spec$(S) \to$ Spec(R) *is continuous.*

Proof. Note that if $\mathfrak{p} \subset S$ is prime, then the lift $\phi^{-1}(\mathfrak{p})$ is a prime in R containing $\ker \phi$, so we can define $\psi = \phi^{-1}$.

It is sufficient to show that preimage of closed sets is closed. Let $V(I)$ be a closed set in Spec(R). Let $J = \phi^{-1}(I)$ be the lift of I. We claim that $\psi(V(I)) = V(J)$. Indeed, $I \subset \mathfrak{p} \implies J = \phi^{-1}(I) \subset \phi^{-1}(\mathfrak{p})$, so $\psi(V(I)) \subset V(J)$. Conversely, if $\mathfrak{p} \in V(J)$, then $\mathfrak{p} \subset J \subset \ker \phi$, so taking quotient map $\phi(\mathfrak{p})$ is prime containing I, so $\phi(V(J)) \subset V(I)$. Combining these two, we get $\psi(V(I)) = V(J)$ is closed, as required. □

In general, however, Spec(R) is not Hausdorff. In particular, if there exist primes $\mathfrak{p} \subsetneq \mathfrak{q}$, then any open set containing $\mathfrak{q}$ must contain $\mathfrak{p}$, so Spec(R) is in fact not T_1. Thus if Spec(R) is Hausdorff, then all primes are maximal. The converse is partially true:

Theorem 93. *Let* R *be a Noetherian ring. Then* Spec(R) *is Hausdorff iff* R *is Artinian.*

Proof. We already proved that Spec(R) Hausdorff implies all primes are maximal, which means R is Artinian. Conversely, if R is Artinian, then all primes are maximal and there are only finitely many primes, so for any two primes $\mathfrak{m}_1, \mathfrak{m}_2$ out of all primes $\mathfrak{m}_1, \dots \mathfrak{m}_l$ consider the open sets $V(\mathfrak{m}_1\mathfrak{m}_3 \cdots \mathfrak{m}_l)^c$ and $V(\mathfrak{m}_2\mathfrak{m}_3 \cdots \mathfrak{m}_l)^c$, which are precisely $\{\mathfrak{m}_2\}$ and $\{\mathfrak{m}_1\}$, which separate the two primes. □

21 Locally free Modules

Definition. An R-module M is called locally free if for every prime $\mathfrak{p}$, the localized module $M_\mathfrak{p}$ is free.

Assume M is locally free with $M_\mathfrak{p} = R_\mathfrak{p}^{n_\mathfrak{p}}$.

Theorem 94. *If* R *is Noetherian, then the map from* Spec(R) *to* $\mathbb{R}$ *given by* $\mathfrak{p} \to n_\mathfrak{p}$ *is continuous.*

Proof. Let ϕ be this map. If we have $\mathfrak{p} \subset \mathfrak{q}$, then $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}} \implies R_{\mathfrak{p}}^{n_{\mathfrak{p}}} = (R_{\mathfrak{q}})_{\mathfrak{p}}^{n_{\mathfrak{q}}} = R_{\mathfrak{p}}^{n_{\mathfrak{q}}} \implies n_{\mathfrak{p}} = n_{\mathfrak{q}}$ because R is commutative. Now for any $n \in \mathbb{Z}$, consider $\phi^{-1}(n)$. This is closed under subsets and supersets. Hence, if it is non-empty, it is completely described by its set of minimal primes, say $\{\mathfrak{p}_1, \dots \mathfrak{p}_k\}$. These must also be minimal primes in R, so there are only finitely many of them. Now we can easily check that $\phi^{-1}(n) = V(\mathfrak{p}_1 \cdots \mathfrak{p}_k)$, so it is closed. Further, since there are only finitely many minimal primes in R, $\operatorname{Im}(\phi)$ is finite. Therefore any closed set in $\operatorname{Im}(\phi)$ is a finite set, and hence its pre-image is a finite union of closed sets, and so is also closed. Therefore ϕ is continuous. □

22 Completion of Rings

Let I be an ideal of a ring R, and let M be an R-module. We can define a pseudo-metric on M using I as follows: For any $x, y \in M$, let n be the largest non-negative integer satisfying $x - y \in I^n M$ (with $I^0 = R$); then $d(x, y) = 2^{-n}$. This pseudo-metric defines the I-adic topology on M.

Theorem 95. *Let R, S be rings, $I \subset R$ be an ideal, and $\phi : R \to S$ be a ring homomorphism. Then ϕ is continuous w.r.t. the I-adic topology on R and $\phi(I)$-adic topology on S.*

Proof. Let $x_1, x_2, \dots$ be a sequence in R converging to some a. Then for any $n > 0$, for all large k we have $a - x_k \in I^n \implies \phi(a) - \phi(x_k) \in \phi(I)^n \implies \phi(x_1), \phi(x_2), \dots$ converges to $\phi(a)$ in S. Therefore ϕ is continuous. □

Theorem 96. *Let M, N be R-modules, $I \subset R$ be an ideal, and $\phi : M \to N$ be an R-module homomorphism. Then ϕ is continuous w.r.t. the I-adic topology on M and I-adic topology on N.*

Proof. The proof is the same as that of the above claim. □

Theorem 97. *In an R-module M, the operations of addition and scalar multiplication are continuous w.r.t. the I-adic topology.*

Proof. We use the above theorem. Simply notice that scalar multiplication induces a linear map from M to M, while addition is a linear map from $M \oplus M$ to M. □

We can then talk about pseudo-metric space completions of these rings and modules. The completion of M is denoted by $\hat{M}$. The completion of a module will be a module, and that of a ring will also be a ring, because we can define product and sum of Cauchy sequences term-by-term. Further, by using constant Cauchy sequences, R sits inside its completion as a subring.

Theorem 98. *Let R be a ring. Then completion of $R[x]$ w.r.t. $\langle x \rangle$-adic topology is $R[[x]]$.*

Proof. Let $p_1, p_2, \dots$ be a Cauchy sequence in $R[x]$. For any $n \geq 0$, there exists an $N(n) > 0$ such that $x^n \mid p_i - p_j$ for every $i, j > N(n)$. Associate with every such Cauchy sequence the power series $a_0 + a_1 x + \cdots$ given by $a_0 + a_1 x + \cdots a_n x^n = p_i \pmod{x^n}$ for any $i > N(n)$. If two Cauchy sequences $\{p_i\}$ and $\{q_j\}$ are in the same equivalence class, then for any m and large n, $x^m \mid p_n - q_n$, so the power series given by both of them is the same. Thus this association is well-defined. Further, we can easily see that usual notions of addition and product go through to power series. □

In the same way, we can prove that completion of $\mathbb{Z}$ or $\mathbb{Q}$ w.r.t. the p-adic metric for any prime p is the set of p-adic integers $\mathbb{Z}_p$ or p-adic rationals $\mathbb{Q}_p$ respectively.

Of course, the completion of a ring must remain complete.

Theorem 99. *Let R be a ring with an ideal I. Let J be the completion of I w.r.t. I-adic pseudo-metric. Then $\hat{R}$ is complete w.r.t. the J-adic topology.*

Proof. It is enough to show that the usual notion of metric in a completion and the J-adic pseudo-metric match. Let $[\{a_{1,i}\}]$ and$[\{a_{2,i}\}]$ be two elements in $\hat{R}$ (here each $\{a_i\}$ is a Cauchy sequence in R). Suppose 2^{-n} is the J-adic distance between them. Then $[\{a_{1,i} - a_{2,i}\}] \in J^n$. Therefore there exists a sequence Cauchy sequence $\{b_i\}$ in I^n such that $\{a_{1,i} - a_{2,i}\} \sim \{b_i\}$, i.e., for any $m > 0$, $a_{1,i} - a_{2,i} - b_i \in I^m$ for all large i. Therefore for all large k, $a_{1,k} - a_{2,k} \in I^n$. Therefore the usual completion distance between $[\{a_{1,i}\}]$ and $[\{a_{2,i}\}]$ is at most 2^{-n}.

Now, if the distance was some $m \geq n$, then for all large k we have $a_{1,k} - a_{2,k} \in I^m$. Let $c_k = a_{1,k} - a_{2,k}$ for large k, and $c_k \in I^m$ arbitrary for small k. Then we can see that $\{a_{1,i} - a_{2,i}\} \sim \{c_i\}$, so $[\{a_{1,i} - a_{2,i}\}] \in J^m$, so $m \leq n$.

Therefore the two distances are the same, and hence $\hat{R}$ is complete. □

Theorem 100. *Let R be an I-complete ring for some ideal $I \subset R$. Then any quotient R/J is $(I+J)/J$ complete.*

Proof. Let $a_1 + J, a_2 + J \ldots$ be a Cauchy sequence in R/J (w.r.t. $(I+J)/J$ pseudo-metric. Then for any $n > 0$, for all large k $a_k - a_{k+1} + J \in (I^n + J)/J$. That is, there is a sequence $b_k \in J$ such that for any $n > 0$, for all large k we have $a_k - a_{k+1} + b_k \in I^n$. Let $c_1 = b_1$ and $c_{k+1} = c_k - b_k$ for $k \geq 1$. Clearly all $c_k \in J$. Then, $(a_k + c_k) - (a_{k+1} + c_{k+1}) = a_k - a_{k+1} + b_k \in I^n$. Thus by completion of R, the sequence $\{a_k + c_k\}$ converges, say to some d. Then $\{a_k + J\}$ converges to $d + J$, as required. □

We have a special case of a complete ring:

Theorem 101. *Let $(R, \mathfrak{m})$ be a local Artinian ring. Then R is complete w.r.t. the $\mathfrak{m}$-adic topology.*

Proof. $\mathfrak{m}$ is nilpotent, so any Cauchy sequence is eventually constant. □

Using this, we can generalize the existence of coefficient fields:

Theorem 102. *Let $(R, \mathfrak{m})$ be a complete local ring, such that $\bigcap_{n\geq 0} \mathfrak{m}^n = \{0\}$, and some non-zero subfield is a subring of R. Then there exist a field $k \cong R/\mathfrak{m}$ embedded as a subring of R.*

Proof. The proof is similar to the case of R being Artinian. Let k be a maximal subfield contained in R. Existence of such a subfield is guaranteed by Zorn's lemma. Assume $k \neq R/\mathfrak{m}$. Let a be a unit not in k. Then $k[a]$ is not a field, so there exists a minimal polynomial $f \in k[x]$ of a; i.e., $f(a)$ is not zero, and neither a unit, i.e., $f(a) \in \mathfrak{m} \setminus \{0\}$. Choose an $a \notin k$ with minimum possible degree of its minimal polynomial.

We will construct a sequence $a = a_1, a_2, a_3, \ldots$ with $a_{i+1} - a_i \in \mathfrak{m}^i$ for all i, such that f is the minimal polynomial of each a_i, and $f(a_i) \in \mathfrak{m}^i$ for each i. Indeed, assume we have constructed this sequence up to some a_i ($i = 1$ case was already given). Expanding modulo $\mathfrak{m}^{i+1}$, we get $f(a_i + t) \equiv f(a_i) + tf'(a_i) \pmod{\mathfrak{m}^{i+1}}$, for any $t \in \mathfrak{m}^i$. Since no minimal polynomial has degree less than $\deg f$, $f'(a_i)$ must be a unit. Hence in the above, we can take $t = -\frac{f(a_i)}{f'(a_i)} \in \mathfrak{m}^i$, and $a_{i+1} = a_i + t$ to get $f(a_{i+1}) \in \mathfrak{m}^{i+1}$. Since degree of minimal polynomial of a_{i+1} is at least $\deg f$, f must be the minimal polynomial of a_{i+1}, as required.

Note that this $\{a_i\}$ is a Cauchy sequence, so by completeness it must converge to some b. Further, we have $b - a \in \mathfrak{m}$, and since f is continuous, $f(b) \in \bigcap_{n\geq 0} \mathfrak{m}^n = \{0\} \implies f(b) = 0$. We claim that $k[b]$ is a field. Indeed, f has to be the minimal polynomial of b by minimality of degree of f. Therefore $k[b]$ is a proper algebraic extension of k, which contradicts maximality of k. Therefore $k \cong R/\mathfrak{m}$. □

Note: By Artin-Reiss lemma, it can be shown that $\bigcap_{n\geq 0} \mathfrak{m}^n = \{0\}$ if $(R, \mathfrak{m})$ is Noetherian local.