Notes on Atiyah & MacDonald's *Commutative Algebra*

Aditya Dwarkesh

Rings & Ideals

Definition. *A ring R is a set with two binary operations (addition and multiplication) such that*

1. *R is an abelian group with respect to addition*
2. *Multiplication is associative and distributive over addition*

$S \subseteq R$ is a subring of R if S is closed under addition and multiplication, and contains the multiplicative identity.

Note: Henceforth, by *ring* we shall mean a nonzero ring which is both commutative with respect to multiplication, and has a multiplicative identity. We call the multiplicative identity 1 and the additive identity 0.

A ring can be seen as either a generalization of fields, or a generalization of the integers. The term 'ring' was first used by David Hilbert in the context of the set of algebraic integers (an algebraic integer is a complex root of some monic polynomial whose coefficients are integers), in order to suggest that elements had the property of 'circling back' to themselves. For instance, if $a^3 - 4a + 1 = 0$, then in general, it can be seen that a^n is going to be an integral linear combination of 1, a, and a^2 alone.

Definition. *A ring homomorphism, f, is a mapping of a ring A to a ring B such that*

1. *f(x+y)=f(x)+f(y)*
2. *f(xy)=f(x)f(y)*
3. *f(1)=1*

A ring homomorphism preserves *structure*, in the sense that the additional features (the operations) of the domain are mapped to something equivalent in the codomain. The word comes from the Ancient Greek words *homos* ('same') and *morphe* ('shape').

Definition. *An ideal I of a ring R is a subset such that (I, +) is subgroup of (R, +) and $IR \subseteq I$.*
We denote by (x) the ideal Rx; such ideals which are generated by one element are called principal ideals.

An ideal tells us which elements we must identify with 0 (or, equivalently, the precise manner in which we must wrap a ring around itself and thereby reidentify its elements) in order to modulo the ring with a subset and obtain a quotient.

Theorem 1.1 (The Correspondence Theorem)**.** *There is a one-to-one order-preserving correspondence between the ideals J of R which contain I, and the ideals $\bar{J}$ of the quotient ring R/I, given by $J = \phi^{-1}(\bar{J})$, where $\phi(x) = x + I$.*

Proof. 1. **Well-defined:** It is easy to see that J is an ideal. Furthermore, since $\bar{J}$ is an ideal, $\bar{0} \in \bar{J} \implies I \subset J$, since $\phi(I) = \bar{0}$. Therefore, for every ideal $\bar{J} \subseteq R/I, \phi^{-1}(\bar{J})$ is an ideal in R containing I.

2. **Bijective:** Suppose $\phi^{-1}(\bar{J}_1) = \phi^{-1}(\bar{J}_2)$. $x + I \in \bar{J}_1 \implies x \in \phi^{-1}(\bar{J}_1) \implies x \in \phi^{-1}(\bar{J}_2) \implies x + I \in \bar{J}_2 \implies \bar{J}_1 = \bar{J}_2$ by symmetry; and so the map is injective.
Let J be an ideal in R containing I, and consider $\bar{J} = \{x + I | x \in J\}$. It is clear that $\bar{J}$ is an ideal, and that $J = \phi^{-1}(\bar{J})$; and so the map is surjective.

3. **Order-preserving:** $J \subseteq I \iff \phi^{-1}(\bar{J}) \subseteq \phi^{-1}(\bar{I}) \iff \bar{J} \subseteq \bar{I}$.

□

Some useful concepts:

- A *zero divisor, x,* in a ring is an element which "divides 0" in the sense that $\exists y \neq 0$ such that $xy = 0$.
- A ring with no zero divisors is an *integral domain* (such as $\mathbb{Z}$).
- An element is *nilpotent* if $\exists n \in \mathbb{N}$ such that $x^n = 0$. Any nilpotent element is a zero divisor (but not conversely).
- An element which has a multiplicative inverse is called a *unit.*
- If every element in a ring is a unit, we call it a *field.*
- An integral domain in which every ideal is principal is called a *principal ideal domain.*

Theorem 1.2. *Let R be a ring. Then, the following are equivalent:*

1. *R is a field*
2. *the only ideals in R are 0 and R*
3. *every homomorphism of R into a non-zero ring S is injective*

Proof. *i)* $\implies$ *ii)* and *ii)* $\implies$ *iii)* are simple enough; I only document *iii)* $\implies$ *i).*
Suppose $x \in R$ such that x is not a unit. Then $(x) \neq (1); S = R/(x) \neq 0$. Let $\phi : R- > S$ be the natural homomorphism. By assumption, ϕ is injective $\implies ker(\phi) = 0 = (x) \implies x = 0 \implies R$ is a field. □

Definition. *An ideal $P \subset R$ is prime if $P \neq R$ and $xy \in P \implies x \in P$ or $y \in P$.*
An ideal $M \subset R$ is maximal if $M \neq R$ and $M \subset I \subseteq R \implies I = R$ (where the inclusion $M \subset I$ is strict).

The notion of a prime ideal, say the authors, is the central and fundamental one in commutative algebra. They generalize the primes of arithmetic and the points of geometry. Therefore, it would be nice to know that there is always a 'sufficient supply' of them. This is exactly what theorem 1.4 will tell us.

Theorem 1.3. *Let R be a ring.*

1. *P is prime $\iff$ R/P is an integral domain*
2. *M is maximal $\iff$ R/M is a field*

Proof. First, suppose P is a prime ideal. Let $\bar{x}, \bar{y} \in R/P, \bar{xy} = 0$. Then $xy \in P \implies x \in P$ or $y \in P \implies \bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$, and so R/P is an integral domain.
Next, suppose R/P is an integral domain, and suppose $xy \in P$. Then $\bar{xy} = \bar{0} \implies \bar{x} = \bar{0}$ or $\bar{y} = \bar{0} \implies x \in P$ or $y \in P$, and so P is prime.
Next, suppose M is a maximal ideal, and let $\bar{x} \in R/M \neq \bar{0} \implies x \notin M$. Consider the ideal $I := \{a + rx | a \in M, r \in R\}$. Since $m \subset I, m \neq I$, we have $I = R \implies a + rx = 1$ for some $a, r \implies a + \bar{rx} = \bar{1} \implies \bar{rx} = \bar{1} \implies rx = 1 \implies x$ is a unit, and so R/M is a field.
Next, suppose R/M is a field. Suppose $M \subset I \subseteq R$, and pick $y \in I - M \implies \bar{y} \neq \bar{0}$. Therefore, $\exists \bar{z}$ such that $\bar{yz} = \bar{1} \implies 1 - yz \in m \subset I \implies 1 \in I$, since $yz \in I$. Therefore, $I = R$, and so M is a maximal ideal. □

Theorem 1.4. *Every ring R has at least one maximal ideal.*

Proof. Let Σ be the set of all ideals $I \neq R$. $0 \in \Sigma \implies \Sigma \neq \emptyset$. Order Σ by inclusion, making it a partially ordered set. We shall show that every chain in Σ has an upper bound.
Let I_α be a chain of ideals in Σ. Then, $I = \bigcup_\alpha I_\alpha$ is an upper bound of the chain: I is (clearly) an ideal which includes each one of the others, and $1 \notin I$ because $1 \notin I_\alpha \forall \alpha$.
Thus, by Zorn's lemma, Σ has a maximal element. This is the required maximal ideal. □

Corollary 1.4.1. *If $I \neq R$ is an ideal of R, there exists a maximal ideal of R containing I.*

Proof. Apply theorem 1.4 to R/I, and then use theorem 1.1.

Corollary 1.4.2. *Every non-unit of R is contained in a maximal ideal.*

Proof. If x is a non-unit, consider (x). If this is maximal, we are done. If not, it is contained in some maximal ideal, and we are once again done.

Definition. *A ring with exactly one maximal ideal is called a local ring, and the field R/M is called the residue field of R.*
A ring with finitely many maximal ideals is called semi-local.

Local rings often arise due to a certain process of 'localizing a ring' at a prime ideal. We will see this in detail in section 3.

Theorem 1.5. *Let R be a ring.*

1. *If $M \neq R$ is an ideal such that every $x \in R - M$ is a unit, then R is a local ring and M is its maximal ideal.*
2. *If M is a maximal ideal such that every element $x \in 1 + M$ is a unit, then R is a local ring.*

Proof. 1. Every ideal $I \neq R$ consists only of non-units. Therefore, $I \subseteq M$ for every ideal, and M is the unique maximal ideal.

2. Let $x \in R - M$. By maximality of $M, (x, M) = R \implies xy + t = 1$ for some $y \in R, t \in M \implies xy = 1 - t \in 1 + M \implies xy$ is a unit $\implies x$ is a unit. It follows now from 1 that R is a local ring.

□

Definition. *The set of all nilpotent elements N of a ring R is called the nilradical of R.*

Theorem 1.6. *The nilradical of a ring is an ideal, and R/N has no nonzero nilpotent element.*

Proof. $x \in N \implies ax \in N$. Also, $x^n = 0, y^m = 0 \implies (x + y)^{m+n-1} = 0$. Thus, N is an ideal.
Let $\bar{x} \in R/N$. $\bar{x}^n = 0 \implies x^n \in N \implies x \in N \implies \bar{x} = \bar{0}$. □

Theorem 1.7. *The nilradical of R is the intersection of all the prime ideals of R.*

Proof. $x \in N \implies x^n = 0 \in P$ for every prime ideal $P \implies x \in P$ for every prime ideal $P \implies N \subseteq \bigcap_\alpha P_\alpha$.
To prove $\bigcap_\alpha P_\alpha \subseteq N$ we show that $x \notin N \implies x \notin P$ for some prime ideal P.
Pick an $x \notin N$ and let $\Sigma = \{I | x^n \notin I \ \forall n \in \mathbb{N}\}$. $0 \in \Sigma \implies \Sigma \neq \emptyset$. That Zorn's lemma is applicable can be seen by a construction similar to 1.4. Therefore, Σ has a maximal element P. It is clear by the construction that $x \notin P$. We claim that this is also a prime ideal, that is, $a, b \notin P \implies ab \notin P$.
$a, b \notin P \implies P \subset P + (a), P \subset P + (b)$ strictly $\implies P + (a), P + (b) \notin \Sigma$. By the definition of $\Sigma, x^m \in P + (a), x^n \in P + (b) \implies x^{mn} \in P + (ab) \implies P + (ab) \notin \Sigma \implies ab \notin P$, and so P is a prime ideal. This completes the proof. □

Definition. *The intersection of all the maximal ideals of a ring R is called the Jacobson radical J of R.*

Remark. It is clear that the Jacobson radical will always contain the nilradical, since every maximal ideal is also prime.

Theorem 1.8. *$x \in J \iff 1 - xy$ is a unit for all $y \in R$.*

Proof. First, suppose $x \in J, 1 - xy$ is not a unit for some y. By 1.4.2, it belongs to some maximal ideal M. $x \in J \subseteq M, y \in M \implies xy \in M \implies 1 \in M$, a contradiction. Thus, $1 - xy$ is a unit for all $y \in R$.
For the converse, $x \notin J \implies x \notin M$ for some maximal ideal M. This gives $M \subset M + (x) = R \implies 1 = u + xy, u \in M, y \in R \implies 1 - xy = u \in M \implies 1 - xy$ is not a unit. □

Definition. *Let R be a ring and I, J be ideals.*

1. *$I+J=\{x+y|x\in I, y\in J\}$ is an ideal. I and J are said to be coprime if $I+J=R$.*
2. *$I\cap J$ is an ideal.*
3. *$IJ=\{\sum_i x_iy_i|x_i\in I, y_i\in J\}$ is an ideal.*

Remark: $I\cup J$ is not, in general, an ideal.

It is clear that the set of all ideals will be partially ordered under inclusion; further, the supremum of any subset of ideals will be given by their sum, and the infimum of any subset of ideals will be given by their intersection. By the above, both will be contained in the parent set. Thus, the ideals of a ring form a *complete lattice* with respect to inclusion.

Lemma 1.9. 1. *I(J+K)=IJ+IK (Distributive law)*

2. *I∩(J+K)=I∩J + I∩K if $J\subseteq I$ or $K\subseteq I$ (Modular law)*

Definition. *The direct product of the rings $R_1, R_2...R_n$ is a ring $\Pi_{i=1}^n R_i$, is the set of all sequences $(x_1,...x_n)$ such that $x_i\in R_i$ with componentwise addition and multiplication.*

Theorem 1.10. *Define $\phi: R\to \Pi_{i=1}^n R/I_i$, $\phi(x)=(x+I_1,...x+I_n)$. Then:*

1. *If I_i, I_j are coprime for $i\neq j$, $\Pi I_i=\bigcap I_i$*
2. *ϕ is surjective $\iff$ I_i, I_j are coprime for $i\neq j$*
3. *ϕ is injective $\iff$ $\bigcap I_i=(0)$.*

Proof. 1. By induction on n.
$n=2$: It is clear that always, $IJ\subseteq I\cap J$. On the other hand, if I, J are coprime, there exists $x\in I, y\in J$ such that $x+y=1$. Suppose $a\in I\cap J \implies a=a.1=a(x+y)=ax+ay \implies a\in IJ \implies I\cap J\subseteq IJ$, and we are done.
Next, suppose this is true for $I_1,...I_{n-1}$, and let $J=\Pi_{i=1}^{n-1} I_i=\bigcap_{i=1}^{n-1} I_i$. If we can show $J+I_n=R$, we are done.
Now, $I_i+I_n=R \implies x_i+y_i=1$ for some $x_i\in I_i, y_i\in I_n \forall I_i$. $(x_1,...x_{n-1})=((1-y_1),...(1-y_{n-1}))$. But now note that $\Pi_{i=1}^{n-1}(1-y_i)-1\in I_n$, because each term except the first 1 in the product expanded will have some y_i factors. Thus, $1\in J+I_n \implies J+I_n=R$.

2. Suppose ϕ is surjective. Without loss of generality, we show that I_1, I_2 are coprime. By assumption, $\exists x\in R$ such that $\phi(x)=(1,0,...0) \implies \phi(x-1)=(0,-1,...-1) \implies x-1\in I_1$. Similarly, $x\in I_2$. Thus, $(1-x)+x=1\in I_1+I_2$, and we are done.
Next, suppose I_i, I_j are coprime for $i\neq j$. It suffices to show that $\exists x\in R$ such that $\phi(x)=(1,0...0)$, since the proof can be repeated for any $(0,...1,...0)$, and the product ring is generated by these.
We have $x_i+y_i=1, x_i\in I_1, y_i\in I_i, i>1$. Define $x=\Pi_{i=2}^n y_i=\Pi_{i=2}^n(1-x_i) \implies x-1\in I_1, x\in I_i \forall i>2$. Thus, $\phi(x)=(1,0,...0)$.

3. Follows directly from the fact that $\ker(\phi) = \bigcap I_i$.

□

Theorem 1.11. *Let R be a ring, $P, P_1, ...P_n$ be prime ideals and $I, I_1, ...I_n$ be ideals.*

1. *$I \subseteq \bigcup_{i=1}^n P_i \implies I \subseteq P_i$ for some i.*
2. *$\bigcap_{i=1}^n I_i \subseteq P \implies I_i \subseteq P$ for some i, and $\bigcap_{i=1}^n I_i = P \implies I_i = P$ for some i.*

Proof. 1. We show $I \nsubseteq P_i$ for any $i \implies I \nsubseteq \bigcup_{i=1}^n P_i$ by induction on n.
$n = 1$: This is trivially true.
Suppose this is true for $n-1$ ideals. Then, $I \nsubseteq P_i$ for $i \in \{1, ...n\} \implies I \nsubseteq \bigcup_{i \in K} P_i$, where $K \subseteq \{1, ...n\}, |K| = n-1$. So for each i, we can find an $x_i \in I, x_i \notin P_j$ for $j \neq i$ by excluding P_i from the union.
If we have $x_i \notin P_i$ for any i, we get $x_i \notin P_i \forall i \in \{1, ...n\}$ and we are done. Suppose, then, $x_i \in P_i$ for all i, and define $y = \sum_{i=1}^n x_1 x_2 ... x_{i-1} x_{i+1} ... x_n$. Then $y \in I, y \notin P_i$ for all i, since each term of the summation is not in a particular P_i, and we have $I \nsubseteq \bigcup_{i=1}^n P_i$.

2. $I_i \nsubseteq P$ for all $i \implies \exists x_i \in I_i, x_i \notin P \implies \Pi x_i \in \Pi I_i \subseteq \bigcap_{i=1}^n I_i$, but $\Pi x_i \notin P$, since P is prime and $x_i \notin P$ for each x_i. Thus, $\bigcap_{i=1}^n I_i \nsubseteq P$.
Also, $P = \bigcap_{i=1}^n I_i \implies P \subseteq I_i \forall i$. But also, $\Pi I_i \subseteq \bigcap I_i \implies \Pi I_i \subseteq P \implies I_i \subseteq P$ for some i. Thus, $P = I_i$ for some i.

□

Definition. *Let I, J be ideals and R be a ring.*

1. *The ideal quotient of I, J is defined as $(I : J) = \{x \in R : xJ \subseteq I\}$.*
   The annihilator of I is $(0 : I)$, denoted by $Ann(I)$.
   The zero divisor of R can be written as $D = \bigcup_{x \neq 0} Ann((x))$.
2. *The radical of I is defined as $r(I) = \{x \in R : x^n \in I, n \in \mathbb{N}\}$. Alternatively, $r(I) = \phi^{-1}(N_{R/I})$, where ϕ is the standard homomorphism from R to R/I.*

It is easy to see that the ideal quotient is an ideal. It arises in the description of the set difference in algebraic geometry. That the radical is also an ideal follows from the fact that the nilradical $N_{R/I}$ is an ideal. We can define the radical of any subset E of R in the same way. However, it will not, in general, be an ideal. The radical of an ideal has a characterization in terms of prime ideals similar to the nilradical.

Theorem 1.12. *Let R be a ring and I, J be ideals.*

1. *$r(I)$ is the intersection of all the prime ideals containing I.*
2. *$D = \bigcup_{x \neq 0} r(Ann((x)))$.*
3. *$r(I), r(J)$ are coprime $\implies I, J$ are coprime.*

Proof. 1. By 1.7, $N_{R/I}$ is the intersection of all the prime ideals in R/I containing it, so that $N_{R/I} = \bigcap P_\alpha$. $r(I) = \phi^{-1}(N_{R/I}) = \phi^{-1}(\bigcap P_\alpha) = \bigcap \phi^{-1}(P_\alpha) = \bigcap P_\beta$, since the

preimage of a prime ideal is also prime. $N_{R/I} \subseteq P_\alpha \implies r(I) \subseteq P_\beta$, and we are done. That every prime ideal containing $r(I)$ will be a part of this intersection follows from the correspondence theorem.

2. $ax = 0 \implies a^n x = 0 \forall n \in \mathbb{N}$. Thus, $a \in D \implies a \in r(D) \implies D \subseteq r(D)$. Next, suppose $a \in r(D) \implies a^n x = 0, n \in \mathbb{N} \implies a(a^{n-1}x) = 0 \implies a \in Ann((x)) \implies a \in D \implies r(D) \subseteq D$, and so $D = r(D)$.

   $x \in r(\bigcup_\alpha E_\alpha) \implies x^n \in \bigcup_\alpha E_\alpha \implies x^n \in E_\alpha$ for some $\alpha \implies x \in \bigcup_\alpha r(E_\alpha)$, and so $r(\bigcup_\alpha E_\alpha) \subseteq \bigcup_\alpha r(E_\alpha)$. On the other hand, $x \in \bigcup_\alpha r(E_\alpha) \implies x \in r(E_\alpha)$ for some $\alpha \implies x^n \in E_\alpha \implies x^n \in \bigcup_\alpha E_\alpha \implies x \in r(\bigcup_\alpha E_\alpha) \implies \bigcup_\alpha r(E_\alpha) \subseteq r(\bigcup_\alpha E_\alpha)$, and so $r(\bigcup_\alpha E_\alpha) = \bigcup_\alpha r(E_\alpha)$.

   Thus, $D = r(D) = r(\bigcup_{x \neq 0} Ann((x))) = \bigcup_{x \neq 0} r(Ann((x)))$.

3. We show that $r(I) = R \iff I = R$ and that $r(I + J) = r(r(I) + r(J))$. Then, $r(I + J) = r(r(I) + r(J)) = r(R) = R \implies I + J = R$, and we are done.
   It is obvious that $I = R \implies r(I) = R$. Suppose $r(I) = R \implies 1 \in r(I) \implies 1 \in I \implies I = R$.
   Next, $x \in r(I + J) \implies x^n \in I + J \implies x^n = i + j \implies x^n \in r(I) + r(J)$, since $i \in r(I), j \in r(J) \implies x \in r(r(I) + r(J)) \implies r(I + J) \subseteq r(r(I) + r(J))$. On the other hand, $x \in r(r(I) + r(J)) \implies x^n \in r(I) + r(J) \implies x^n = i + j, i^m \in I, j^k \in J \implies x^r \in I + J$ for some high enough $r \implies x \in r(I + J) \implies r(r(I) + r(J)) \subseteq r(I + J)$, and we are done.

□

Definition. *Let $f : R \to S$ be a homomorphism and I, J be ideals in R and S respectively.*

1. *The extension of I, I^e, is the ideal in S generated by f(I).*
2. *The contraction of J, J^c, is the ideal $f^{-1}(J)$ in R.*

f can be factored as $A \xrightarrow{p} f(A) \xrightarrow{j} B$.
p is surjective (its action is basically that of f), and there is a one-one correspondence between ideals of $f(A)$ and ideals of A which contain ker(f); prime ideals correspond to prime ideals.
j is injective (its action is to multiply $f(A)$ with B). The behaviour of prime ideals under extensions of this sort is one of the central problems of algebraic number theory.

Example. Consider $\mathbb{Z} \to \mathbb{Z}[i]$. If $p \equiv 1 (\text{mod } 4)$, then $(p)^e$ is the product of two distinct prime ideals (say, $(5)^e = (2 + i)(2 - i)$). This is equivalent to Fermat's theorem on sums of two squares.

Theorem 1.13. *Let $f : R \to S$ be a homomorphism and I, J be ideals in R and S respectively.*

1. $I \subseteq I^{ec}, J^{ce} \subseteq J$
2. $J^c = J^{cec}, I^e = I^{ece}$
3. $C = \{J^c | J \text{ is an ideal of } S\} = \{I | I^{ec} = I\}$, $E = \{I^e | I \text{ is an ideal of } R\} = \{J | J^{ce} = J\}$; $F : C \to E, F(I) = I^e$ *is bijective and* $F^{-1} : E \to C \equiv F^{-1}(J) = J^c$.

Proof. 1. $x \in I \implies x \in f^{-1}(f(I)) \implies I \subseteq I^{ec}$.
$x \in J^{ce} \implies x \in f(f^{-1}(J)) \implies f^{-1}(x) \in f^{-1}(J) \implies x \in J \implies J^{ce} \subseteq J$.

2. We know from 1 that $J^c \subseteq J^{cec}$. But also, $J^{ce} \subseteq J \implies J^{cec} \subseteq J^c$, and therefore $J = J^{cec}$.
The proof runs similarly for $I^e = I^{ece}$.

3. $I \in C \implies I = J^c, J$ is some ideal of S. But $J^c = J^{cec} \implies I = I^{ec}$. Conversely, $I^{ec} = I \implies I = J^c$, where $J = I^e$, and we are done.
The proof runs similarly for E.
F is surjective: For any ideal J, set I=J^c.
F is injective: $F(I_1) = F(I_2) \implies I_1^e = I_2^e \implies I_1^{ec} = I_2^{ec} \implies I_1 = I_2$.

□

Remark. E is closed under sum and product. C is closed under intersection and radicalization.

Exercises

Prime spectrum of a ring:

Let R be a ring, X be the set of all prime ideals of R, and $V(E)$ the set of all prime ideals of R which contain E for any $E \subseteq R$. Consider the collection of sets $\tau = \{V(E) | E \subseteq R\}$.

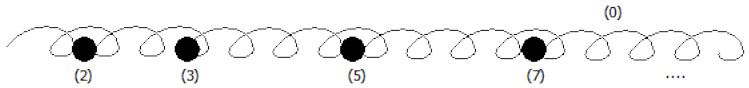
$X, \emptyset \in \tau$: It is clear that $V(R) = \emptyset, V(0) = X$.

τ is closed under arbitrary intersection: $P \in V(\bigcup_{i\in\lambda} E_i) \iff (\bigcup_{i\in\lambda} E_i) \subseteq P \iff E_i \subseteq P$ for all $i \iff P \in V(E_i) \forall i \iff P \in \bigcap_{i\in\lambda} V(E_i)$.

τ is closed under finite union: $P \in V(IJ) \iff IJ \subseteq P \iff I \subseteq P$ or $J \subseteq P \iff P \in V(I) \cup V(J)$; and so $V(I) \cup V(J) = V(IJ)$.
Next, $IJ \subseteq I \cap J \implies (I \cap J \subseteq P \implies IJ \subseteq P)$. But $I \cap J \subseteq P \iff P \in V(I \cap J)$, and so $V(I \cap J) \subseteq V(IJ)$. On the other hand, $P \in V(IJ) \implies IJ \subseteq P \implies I \subseteq P$ or $J \subseteq P \implies I \cap J \subseteq P \implies P \in V(I \cap J)$, and so $V(IJ) = V(I \cap J)$.

Therefore, (X, τ) form a topological space, where the collection τ gives us the closed sets of the space. This topological space is called the prime spectrum of R, written as Spec(R). The topology itself is called the *Zariski topology*. It is in this sense that a prime ideal shows up as a point in a space.

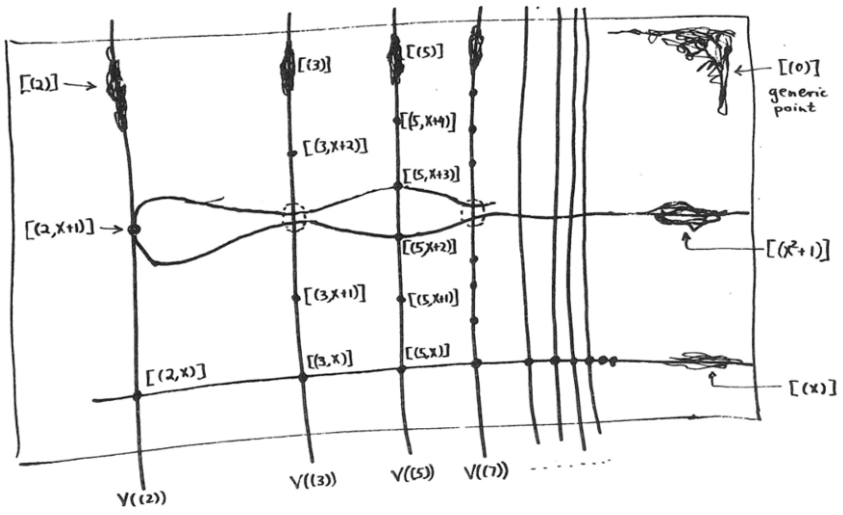
Example. In the Zariski topology on $\mathbb{Z}$, the points are (0) and (p). (p) are all closed sets by virtue of the fact that $(p) = V((p))$. Thus, in the prime spectrum of $\mathbb{Z}$, the closed sets are finite unions of the singletons (except (0)), the null set, and the whole space. Image from Wikipedia.



In case of $\mathbb{R}$ (or any field, really), $X = \{(0)\}$, and there is nothing more to be said.

Finally, consider the ring $\mathbb{Z}[x]$. To describe the elements (points) of its spectrum amounts to describing its prime ideals. Since this is a unique factorisation domain, an element is prime iff it is irreducible. Using this, we can claim that the prime ideals of $\mathbb{Z}[x]$ are of four kinds: (0), (p), where p is a prime integer, (f), where f is an irreducible polynomial, and (p, f), where p is a prime integer and f is an irreducible polynomial in $\mathbb{Z}[x]/(p)$ (full proof).

The following image of it with the Zariski topology is drawn by David Mumford, and is presently incomprehensible to me.



Affine algebraic varieties:

Let K be an algebraically closed field, and let $f_\alpha(t_1, ..., t_n) = 0$ be a set of polynomial equations in n variables with coefficients in K. Define $X = \{(x_1, ...x_n) \in K^n : f_\alpha(x_1, ..., x_n) = 0 \forall \alpha\}$. The set $X \subseteq K^n$ is called an *affine algebraic variety.*

Next, define $I(X) = \{g \in K[t_1, ..., t_n] : g(x) = 0 \forall x \in X\}$. The set $I(X) \subseteq K[t_1, ..., t_n]$ is (clearly) an ideal, called the *ideal of the variety X.*

Consider the quotient $P(X) = K[t_1, ..., t_n]/I(X)$. Two functions g, h are equal in it iff $g - h \in I(X) \iff g = h$ on X. Thus, $P(X) = X[t_1, ...t_n]$, and is called the *coordinate ring* (or affine algebra) of X.

Consider the canonical map $\phi : K[t_1, ..., t_n] \to P(X), \phi(f) = f + I(X)$. Define $\xi_i = \phi(t_i) = t_i + I(X)$. $\{\xi_i\}$ are called the *coordinate functions* on X.

Next, consider the topological space $\mathrm{Spec}(P(X))$, whose points are the prime ideals of $P(X)$. This will have a subspace consisting of the set of maximal ideals of $P(X)$, with the induced topology from the parent space. Call this topological subspace $\mathrm{Max}(P(X)) = \widetilde{X}$.

Finally, define a map between the sets $\mu : X \to \widetilde{X}, \mu(x) = \overline{M_x}$.
$\overline{M_x} = \{f \in P(X) : f(x) = 0\}$ and will be a maximal ideal, because $\overline{M_x}$=ker(h), where $h : P(X) \to K, h(f) = f(x)$, and $P(X)/\ker(h) \cong K \iff \ker(h)$ is a maximal ideal, since K is a field.

μ is a bijection:

1. Injectivity: $x \neq y \implies x_i \neq y_i$ for some $i \implies \xi_i - x_i = 0 \in M_x$, but $\xi_i - x_i \notin M_y$, since $(\xi_i - x_i)(y) = y_i - x_i \neq 0$. Thus, $M_x \neq M_y \implies \mu(x) \neq \mu(y) \implies \mu$ is injective.

2. Surjectivity: We wish to show that every maximal ideal of $P(X)$ is of the form $\overline{M_x}$. We shall prove this by assuming the weak form of Hilbert's Nullstellensatz:

   If an ideal I of $K(t_1, ..., t_n)$ is proper, then the affine algebraic variety associated with it is non-empty.

   Assuming this, let M be a maximal ideal of $K[t_1, ...t_n]$. Then, $Z(M) \neq 0 \implies \exists x \neq 0 : x \in Z(M)$. This means all the polynomials in M vanish at x; and so, we have $M \subseteq M_x$. By maximality, $M = M_x$ (note that $M_x = \{f \in K[t_1, ...t_n] : f(x) = 0\}$). We can thus onclude that every maximal ideal of $K[t_1, ..., t_n]$ is of the form M_x.
   The correspondence theorem tells us that there is a one-one correspondence between maximal ideals of $P(X)$ and maximal ideals of $K[t_1, ...t_n]$ containing $I(X)$, given by $M = \phi^{-1}(\overline{M})$, where ϕ is the canonical map between ring and quotient.
   But we know that every maximal ideal of $K[t_1, ...t_n]$ is of the form M_x. Thus, every maximal ideal of $P(X)$ is of the form $\phi(M_x) = \{f + I(x) : f(x) = 0, f \in K[t_1, ...t_n]\} = \{f \in P(X) : f(x) = 0\} = \overline{M_x}$, and we are done.

Algebraic closure of a field:

A field F is said to be algebraically closed if every non-constant polynomial in $F[x]$ has a root in F.

Let K be a field, and Σ be the set of irreducible monic polynomials f in one variable with coefficients in K.

Let the ring $R = K[x_{f_1}, ...]$, where there is one indeterminate for each function $f_i \in \Sigma$, and define an ideal of R, I, with the generating set $\{f(x_f) | f \in \Sigma\}$.

$I \neq R$: Suppose $1 = \sum_{i=1}^{n} g_i f_i(x_{fi})$. All the polynomials $\{f_i\}$ have a root $\{\alpha_i\}$ in the field extension E_n of K defined inductively by $E_1 = K[x]/(f_1); E_2 = E[x]/(f_2)$, etc. Substituting $x_{fi} = \alpha_i$, we get $1 = 0$, a contradiction.

By corollary 1.4.1, there exists a maximal ideal M of R containing I. Define the field $K_1 = R/M$. $f(x_f) \in M \implies f(\overline{x_f}) = \overline{f(x_f)} = \bar{0}$ in the quotient; therefore, each polynomial f has, in K_1, a root x_f.

Repeat this construction with K_1 in place of K to obtain another field extension K_2, and so on. Define $L = \bigcup_{n=1}^{\infty} K_n$. L is algebraically closed, because any polynomial with coefficients in it has its coefficients in some K_n with sufficiently large n, and so its roots are in K_{n+1}, and hence in the union itself.

Finally, define $\overline{K} \subseteq L$ as those elements in L for which there exists some non-zero polynomial $g(x)$ with coefficients in K such that $g(a) = 0$ (in other words, the set of elements which are algebraic over K). $\overline{K}$ is the algebraic closure of K.

Modules, exact sequences, tensor products

Definition. *An R-module is a pair (M, μ) where M is an abelian group and $\mu : A \times M \to M$ is a map such that for $a, b \in R, x, y \in M$, we have*

1. *a(x+y)=ax+ay*
2. *(a+b)x=ax+bx*
3. *(ab)x=a(bx)*
4. *1x=x*

A map between R-modules $f : M \to N$ is an R-module homomorphism if

1. *f(x+y)=f(x)+f(y)*
2. *f(ax)=af(x)*

Lemma 2.1. *An abelian group (M, +) is a module iff there is a ring homomorphism $A \to E(M)$, where E(M) is the ring of endomorphisms on M.*

Proof. If M is a module, define the homomorphism $\psi : A \to E(M), \psi(a) = \mu_a$, where $\mu_a(x) = ax$. If there is a homomorphism $\psi : A \to E(M)$, define the map $\mu : A \times M \to M, \mu(a, x) = \psi(a)(x) = ax$. □

Example. A module helpfully offers some extra 'elbow-room' when dealing with a ring, and generalizes a number of familiar concepts.

1. An ideal of a ring is a module.
2. A vector space over a field is a module. A homomorphism between modules which are vector spaces is just a linear transformation between vector spaces.
3. Any given abelian group can be seen as a $\mathbb{Z}-$module.
4. The set of all homomorphisms between two modules M and N can itself be turned into a module over the parent ring R, denoted by $\mathrm{Hom}_R(M, N)$. In particular, $\mathrm{Hom}(R, M) \cong M$, since $f : R \to M$ is uniquely determined by $f(1)$.

Remark. A pair of homomorphisms $\mu : M' \to M, \nu : N \to N''$ induce the following mappings:

- $\bar{\mu}$:Hom$(M, N) \to$Hom$(M', N), \bar{\mu}(f) = f \circ \mu$.
- $\bar{\nu}$:Hom$(M, N) \to$Hom$(M, N''), \bar{\nu}(f) = \nu \circ f$.

Some useful concepts:

- A *submodule* N of M is a subgroup of M which is closed under multiplication by R.
- The *quotient* of M by N is the R-module M/N, where $a(x + N) = ax + N$. The natural map from M to M/N is a homomorphism.
- The *kernel* of $f : M \to N$ is the set $\{x \in M : f(x) = 0\}$, and is a submodule of M.

- The *image* of f is the set $f(M)$, and is a submodule of N.
- The *cokernel* of f is $\mathrm{N}/\mathrm{Im}(f)$.
- The *sum* and *intersection* of two modules are defined as they were for ideals.
- The *product* IM of an ideal and a module is the set of all finite sums $\{\sum a_i x_i : a_i \in I, x_i \in M\}$, and is a submodule of M.
- $(N : P) = \{a \in R : aP \subseteq N\}$ for submodules N, P of M is an ideal of R.
- $(0 : M)$ is the *annihilator* of M, denoted by $\mathrm{Ann}(M)$, and is an ideal of R.
- We call the module *faithful* if $\mathrm{Ann}(M) = 0$.

  Remark. For $I \subseteq Ann(M)$, we can regard M as a module over R/I by defining $\bar{x}m = xm$. This is well-defined, since $\bar{x} = \bar{y} \implies x - y \in Ann(M) \implies xm = ym \implies \bar{x}m = \bar{y}m$.
- $\{x_1, ..., x_n, ...\} \subseteq M$ are said to be *generators* of M if any element in M can be expressed as a finite linear combination of them (with coefficients in R).
- A module is *finitely generated* if its set of generators is finite, and *cyclic* if it has a single generator.
- The *direct sum* $\oplus_{i \in I} M_i$ of a family of R-modules consists of the families $(x_i)_{i \in I}, x_i \in M_i$, such that only a finite number of x_i are non-zero.
- The *direct product* $\Pi_{i \in I} M_i$ is defined identically, without the restriction on the x_i. It is an R-module with the operations defined componentwise.
- A *free* module is one which can be written as the direct sum of cyclic modules.

One may wonder why there is a need to define the direct sum and the direct product distinctly, when they are so similar (indeed, identical for a finite family). In a certain sense, however, the two notions are *duals*. While the direct product is a *product* (and this is straightforward enough), the direct sum is what is known in category-theoretic language as a *coproduct*.

Remark. If $R = \Pi_{i=1}^{n} R_i$, we can rewrite it as a module direct sum decomposition $R = I_1 \oplus ... \oplus I_n$, where $I_i = ((0, ...e_i, ...0)), e_i \in R_i$. If we are given this decomposition, we can go back to have $R \cong \Pi_{i=1}^{n}(R/J_i), J_i = \oplus_{j \neq i} I_j$. $I_i \cong R/J_i$.

Lemma 2.2. *$M/ker(f) \cong Im(f)$ for a homomorphism $f : M \to N = Im(f)$.*

Proof. For a submodule M', define $\bar{f} : M/M' \to N$ as $\bar{f}(\bar{x}) = f(x)$. Clearly, $\ker(\bar{f}) = \ker(f)/\mathrm{M}'$. In the case of M'=$\ker(f)$, we have $\ker(\bar{f}) = 0 \implies \bar{f}$ is an isomorphism, which completes the proof.

Theorem 2.3. *Let $L \subset M \subset N$ be R-modules, and M_1, M_2 be submodules of M.*

1. $(L/N)/(M/N) \cong L/M$
2. $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$

Proof. 1. Define $f : L/N \to L/M, f(l + N) = l + M$. Clearly, this is a surjective homomorphism, and $\ker(f) = \{l + N : l \in M\} = M/N$. The result follows from lemma 2.2.

2. Consider $f : M_2 \to (M_1 + M_2)/M_1, f(m_2) = m_2 + M_1$. Clearly, this is a surjective homomorphism, and $\ker(f) = M_1 \cap M_2$. The result follows from lemma 2.2.

□

Theorem 2.4. *M is a finitely generated R-module $\iff$ M is isomorphic to a quotient of R^n for some $n \in \mathbb{N}$.*

Proof. First, suppose M is finitely generated, by $\{x_1, ..., x_n\}$. Define $\phi : R^n \to M, \phi(r_1, ..., r_n) = r_1x_1 + ...r_nx_n$. ϕ is an R-module homomorphism; thus, $M \cong R^n/\ker(\phi)$.
Conversely, suppose $M \cong R^n/I$; we have a surjective (module) homomorphism from R^n to R^n/I, and another one from R^n/I to M. Composing these two, we get a surjective R-module homomorphism $\phi : R^n \to M$. Then, since R^n is generated by $\{e_i\}_{i=1}^n$, M is generated by $\{\phi(e_i)\}_{i=1}^n$, where $e_i = (0, ...1, ...0)$, with the 1 at the i^{th} place. □

Theorem 2.5. *Let M be a finitely generated $R-$module, $I \subseteq R$ be an ideal, and $\phi : M \to M$ be a homomorphism such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation of the following form, for $a_i \in I$:*

$$\phi^n + a_1\phi^{n-1} + ...a_n = 0$$

Proof. Let M be generated by $\{x_1, ..., x_n\}$. $\phi(x_i) \in IM \implies \phi(x_i) = \sum_{j=1}^n a_{ij}x_j, a_{ij} \in I$; and we have the following equation for each $1 \leq i \leq n$:

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0$$

Define a matrix M with entries $m_{ij} = (\delta_{ij}\phi - a_{ij})$. Then, $MX = 0$, where X is the column vector comprised by the x_js. Left-multiplying by adj(M) and using $adj(M)M = det(M)I$, we get $Dx_j = 0 \forall j$, where $D = det(M)$. Thus, the polynomial obtained by expanding out the determinant is a zero endomorphism on M of the required form.

□

Theorem 2.6 (Nakayama's lemma)**.** *We shall prove four interrelated statements, the second of which is known as Nakayama's lemma.*

1. *Let M be a finitely generated $R-$module and $I \subseteq R$ be an ideal such that $IM = M$. Then there exists $x \in 1 + I$ such that $x \in Ann(M)$.*
2. *Let M be a finitely generated $R-$module and $I \subseteq R$ an ideal contained in the Jacobson radical J of the ring. Then $IM = M \implies M = 0$.*
3. *Let M be a finitely generated $R-$module and $I \subseteq R$ be an ideal contained in the Jacobson radical. For any submodule $N \subseteq M$, $M = IM + N \implies M = N$.*
4. *Let R be a local ring, m its maximal ideal, K=R/m its residue field, and M a finitely generated R-module. Then M/mM is a vector space, and M is generated by those elements $\{x_i\}_{i=1}^n$ whose image $\{\phi(x_i)\}_{i=1}^n$ form a basis for M/mM (where ϕ is the natural homomorphism from module to quotient).*

Proof. We prove each of the statements in order.

1. In theorem 2.5, take ϕ = identity. This gives $1 + a_1 + ... + a_n = 0$, and we can set x as equal to this.

2. Two proofs are offered for this.

   - By (1), $\exists x \in 1 + I$ such that $xM = 0$. Since $I \subseteq J, x \in 1 + J \implies x - 1 \in J \implies 1 - (x-1)(-1) = x$ is a unit, by theorem 1.8. Thus, $x^{-1}xM = M = 0$.
   - Suppose $M \neq 0$, and suppose it is generated by $\{x_1, ..., x_n\}$. $x_n \in IM \implies x_n = a_1x_1 + ...a_nx_n, a_i \in I \implies (1 - a_n)x_n = a_1x_1 + ... + a_{n-1}x_{n-1}$.
     But $a_n \in I \implies a_n \in J \implies (1 - a_n)$ is a unit $\implies x_n \in \{x_1, ..., x_{n-1}\}$, a contradiction. Thus, $M = 0$.

3. $x \in I(M/N) \implies x = \sum_{i=1}^n a_i(m_i + N) = \sum_{i=1}^n a_im_i + N \in IM + N \subseteq IM + N + N = (IM + N)/N$. Also, $x \in (IM + N)/N \implies x = \sum_{i=1}^n a_im_i + n + N \implies x = \sum_{i=1}^n a_im_i + N \implies x = \sum_{i=1}^n a_i(m_i + N) \implies x \in I(M/N)$.

   Thus, $I(M/N) = (IM + N)/N$. Next, by assumption, $(IM + N)/N = M/N$. Therefore, we can apply the previous theorem to $M/N \implies M/N = 0 \implies M = N$.

4. We can view M/mM as a K-module, sending $(r + m, x + mM)$ to $rx + mM$. This is well defined, because if $\bar{r} = \bar{r'} \iff r - r' \in m$, $\bar{x} = \bar{x'} \iff x - x' \in mM$, then $rx+mM = rx-r'(x-x')+mM = r'x'+rx-r'x+mM = r'x'+x(r-r')+mM = r'x'+mM$. By being a module over a field, it is a vector space.

   Next, let $N \subseteq M$ be generated by $\{x_i\}_{i=1}^n$.Now, it is clear that $N + mM \subseteq M$, since both of them are submodules of M. Conversely, $x \in M \implies x + mM \in M/mM \implies x + mM = \sum_{i=1}^n k_i\phi(x_i) = \sum_{i=1}^n k_ix_i + mM \implies x - \sum_{i=1}^n k_ix_i \in mM \implies x = \sum_{i=1}^n k_ix_i + z \implies x \in N + mM$, and we are done. Thus, $M = mM + N$.

   Note that m is, in this case, the Jacobson radical; therefore, we can apply (3) to obtain $N = M$, and we are done.

□

Remark. Nakayama's lemma (2) governs the interaction between a ring's Jacobson radical and finitely generated modules. In terms of generators (4), it gives us a more precise sense in which modules over local rings are analogous to vector spaces.

Definition. *A sequence of R-modules and R-homomorphisms*

$$... \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1}...$$

is said to be exact at M_i if Im(f_i)=Ker(f_{i+1}). The sequence is exact if it is exact at each M_i.

Example. The sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact $\iff$ f is injective and g is surjective. By the first isomorphism theorem, $\text{Coker}(f) = M/f(M') = M/ker(g) \cong M''$.
A sequence of this type is called a *short exact sequence.*

Theorem 2.7. *The following statements characterize when a sequence is exact.*

1. $M' \xrightarrow{\mu} M \xrightarrow{\nu} M'' \to 0$ *is exact* $\iff 0 \to Hom(M'', N) \xrightarrow{\bar{\nu}} Hom(M, N) \xrightarrow{\bar{\mu}} Hom(M', N)$ *is exact for all R-modules N.*

2. $0 \to N' \xrightarrow{\mu} N \xrightarrow{\nu} N''$ *is exact* $\iff 0 \to Hom(M, N') \xrightarrow{\bar{\mu}} Hom(M, N) \xrightarrow{\bar{\nu}} Hom(M, N'')$ *is exact for all R-modules M.*

Proof. There are four parts to this proposition.

1. First, suppose the right side sequence in (1) is exact for all modules N. We have to then show two things.

   ν is surjective: Our assumption implies $\bar{\nu}$ is injective $\iff \ker(\bar{\nu}) = 0$. Setting N=Coker$(\nu) = M''/f(M)$, we see that the quotient map $\phi : M'' \to M''/\nu(M)$ is identically zero, since $\bar{\nu}(\phi) = \phi \circ \nu = 0 \implies$ it lies in $\ker(\bar{\nu})$. Thus, $\nu(M) = M'' \implies \nu$ is surjective.

   Im(μ) =Ker(ν): By assumption, $\bar{\mu} \circ \bar{\nu} = 0 \iff f \circ \nu \circ \mu = 0$ for all $f : M'' \to N$. Setting $N = M'', f$ as identity, we have $\nu \circ \mu = 0 \implies$ Im$(\mu) \subseteq$ker(ν). Next, set $N = M/$Im(μ), and $\phi : M \to N$ be the projection. $\bar{\mu}(\phi) = \phi \circ \mu = 0 \implies \phi \in ker(\bar{\mu}) \implies \phi \in Im(\bar{\nu}) \implies \exists \psi : M'' \to N$ such that $\phi = \psi \circ \nu$, so that $x \in ker(\nu) \implies \phi(x) = 0 \iff x \in Im(\mu)$. Thus, $ker(\nu) \subseteq Im(\mu)$, and we are done.

2. Second, suppose the left side sequence in (1) is exact. We have to once again show two things.

   $\bar{\nu}$ is injective: $\bar{\nu}(f) = \bar{\nu}(g) \iff f \circ \nu = g \circ \nu$. But since ν is surjective (by our assumption), we have $f = g$ for all $m'' \in M''$, and we are done.

   Im$(\bar{\nu})$=ker$(\bar{\mu})$: $f \in Im(\bar{\nu}) \implies f = g \circ \nu$ for some $g : M'' \to N$. Now, $\bar{\mu}(f) = f \circ \mu = g \circ \nu \circ \mu = 0$, since $Im(\nu) = ker(\mu)$. Thus, $f \in ker(\bar{\mu}) \implies Im(\bar{\nu}) \subseteq ker(\bar{\mu})$. Next, $f \in ker(\bar{\mu}) \implies f \circ \mu = 0 \implies Im(\mu) \subseteq ker(f) \implies ker(\nu) \subseteq ker(f)$. Now, define $g : M'' \to N, g(m'') = f(m)$, where $m = \nu^{-1}(m'')$. Clearly, $f = g \circ \nu$. We only need to check that g is well-defined; but $\nu(m_1) = \nu(m_2) \implies \nu(m_1 - m_2) = 0 \implies f(m_1 - m_2) = 0 \implies f(m_1) = f(m_2)$, and we are done.

3. Third, suppose the left side sequence (2) is exact.

   $\bar{\mu}$ is injective: $\bar{\mu}(f) = \bar{\mu}(g) \iff \mu \circ f = \mu \circ g \iff \mu(f(x)) = \mu(g(x)) \forall x \in M \iff f(x) = g(x) \forall x \in M$ (since μ is injective by our assumption) $\iff f = g$, and we are done.

   $Im(\bar{\mu}) = ker(\bar{\nu})$: $f \in Im(\bar{\mu}) \implies f = \mu \circ g$, for some $g : M \to N'$. Now, $\bar{\nu}(f) = \nu \circ \mu \circ g = 0$, since $Im(\mu) = ker(\nu)$ (by assumption) $\implies f \in ker(\bar{\nu}) \implies Im(\bar{\mu}) \subseteq ker(\bar{\nu})$. Next, $f \in ker(\bar{\nu}) \implies \nu \circ f = 0 \implies Im(f) \subseteq ker(\nu) \implies Im(f) \subseteq Im(\mu)$. Thus, we can define $g : M \to N', g(m) = \mu^{-1}(f(m))$. Clearly, $f = \mu \circ g$. g is well-defined: $f(m_1) = f(m_2) \implies f(m_1 - m_2) = 0 \implies g(m_1 - m_2) = \mu^{-1}(f(m_1 - m_2)) = 0$, by injectivity.

4. Finally, suppose the right side sequence (2) is exact.

   μ is injective: Let $n' \in N'$ such that $\mu(n') = 0$. Now, pick any element $x \in R$, consider the ideal generated by it, view this ideal as a module and set it as M. Finally, let $f : M \to N'$ be given by $f(x) = n'$. Then $\bar{\mu}(f(x)) = \mu \circ f(x) = \mu(n') = 0 \implies \bar{u}(f) = 0 \implies f \in ker(\bar{\mu}) \implies f = 0 \implies n' = 0$, and so μ is injective.

   $Im(\mu) = ker(\nu)$: $\bar{\nu} \circ \bar{\mu} = 0 \iff \nu \circ \mu \circ f = 0$ for all $f : M \to N'$. Setting $M = N', f = id_{N'}$,

we have $\nu \circ \mu = 0 \implies Im(\mu) \subseteq ker(\nu)$. Finally, let $n \in ker(\nu) \subseteq N$, and let $g : M \to N$ be given by $g(x) = n$, where M is a cyclic module over R (as above). $\bar{\nu}(g)(m) = \nu(g(m)) = \nu(g(rx)) = r\nu g(x) = r\nu(n) = 0, r \in R$; that is, $g \in ker(\bar{\nu}) \implies g \in Im(\bar{\mu}) \implies g = \mu \circ \psi$ for some $\psi : M \to N'$; thus, $n = g(x) = \mu \circ \psi(x) \implies n \in Im(\mu) \implies ker(\nu) \subseteq Im(\mu)$, and we are done.

□

Theorem 2.8 (Snake lemma)**.** *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\mu} & M & \xrightarrow{\nu} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[\mu']{} & N & \xrightarrow[\nu']{} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R-modules and homomorphisms, with the rows exact. Then, there exists an exact sequence

$$0 \to Ker(f') \xrightarrow{\bar{\mu}} Ker(f) \xrightarrow{\bar{\nu}} Ker(f'') \xrightarrow{d} Coker(f') \xrightarrow{\bar{\mu}'} Coker(f) \xrightarrow{\bar{\nu}'} Coker(f'') \to 0$$

in which $\bar{\mu}, \bar{\nu}$ are restrictions of μ, ν and $\bar{\mu}', \bar{\nu}'$ are induced by μ', ν'.

Proof. First, we define the *boundary homomorphism* d as follows: if $x'' \in Ker(f''), x'' = \nu(x)$ for some $x \in M$ (since ν will be surjective), and $\nu'(f(x)) = f''(\nu(x)) = 0 \implies f(x) \in Ker(\nu') = Im(\mu') \implies f(x) = \mu'(y')$ for some $y' \in N'$. Then $d(x'')$ is the image of y' in Coker(f'). Formally, $d(x'') = \phi(\mu'^{-1}(f(\nu^{-1}(x''))))$, where $\phi : N'' \to N'/Im(f')$. The well-definedness of d follows from the injectivity of μ'.

We have a number of things to demonstrate to prove that the sequence given is exact.

- $\bar{\mu}$ is injective: Follows directly from injectivity of μ.
- $Im(\bar{\mu}) = ker(\bar{\nu})$: $x \in Im(\bar{\mu}) \implies x \in Im(\mu) \implies x \in ker(\nu) \implies x \in ker(\bar{\nu}) \implies Im(\bar{\mu}) \subseteq ker(\bar{\nu})$.
  Conversely, $x \in ker(\bar{\nu}) \implies x \in ker(\nu) \implies x \in Im(\mu) \implies x = \mu(m'), m' \in M'$. Now, $\mu'(f'(m')) = f(\mu(m')) = f(x) = 0 \implies f'(m') = 0$ (by injectivity of μ') $\implies m' \in ker(f')$. Thus, $\bar{\mu}(m') = \mu(m') = x \implies x \in Im(\bar{\mu}) \implies ker(\bar{\nu}) \subseteq Im(\bar{\mu})$, and we are done.
- $Im(\bar{\nu}) = ker(d)$: $m'' \in Im(\bar{\nu}) \implies m'' = \bar{\nu}(m), m \in ker(f) \subseteq M$. Now, $f(m) = 0 \implies f(m) = \mu'(0)$, since μ' is injective. Thus, $d(m'') = 0 \implies m'' \in ker(d) \implies Im(\bar{\nu}) \subseteq ker(d)$.
  Next, let $m'' \in ker(d) \subseteq ker(f'') \subseteq M'' \implies m'' = \nu(m)$ for some $m \in M$ by surjectivity of ν. Now, $d(m'') = 0 \implies n' \in Im(f')$, where n' is given by $\mu'(n') = f(m)$. So let $n' = f'(m')$. Since the diagram commutes, $f(\mu(m')) = \mu'(f'(m')) = \mu'(n') = f(m) \implies m - \mu(m') \in ker(f)$. Thus, $\bar{\nu}(m - \mu(m')) = \nu(m) - \nu(\mu(m)) = \nu(m)$ (by exactness of the first row) $= m'' \implies m'' \in Im(\bar{\nu}) \implies ker(d) \subseteq Im(\bar{\nu})$, and we are done.
- $Im(d) = ker(\bar{\mu}')$: Let $\phi' : N \to N/f(M)$ be the quotient map. Then, $\bar{\mu}' \circ d$ $= \bar{\mu}'(\phi(\mu'^{-1}(f(\nu^{-1}(x''))))) = \phi'(\mu'(\mu'^{-1}(f(\nu^{-1}(x''))))) = \phi'(f(\nu^{-1}(x'')) = 0 \implies Im(d) \subseteq ker(\bar{\mu}')$.
  Conversely, suppose $n' + f(M') \in ker(\bar{\mu}') \implies \mu'(n') \in f(M) \implies \mu'(n') = f(m), m \in M$. Set $m'' = \nu(m)$. Then $f''(m'') = f''(\nu(m)) = \nu'(f(m)) = \nu'(\mu'(n')) = 0$ (by exactness

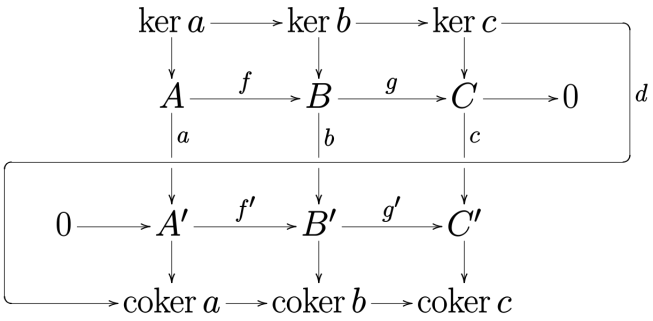
of the sequence) $\implies m'' \in ker(f'')$. Thus, $d(m'') = n' + f(M) \implies n' + f(M) \in Im(d) \implies ker(\bar{\mu}') \subseteq Im(d)$, and we are done.

- $Im(\bar{\mu}') = ker(\bar{\nu}')$: $\bar{\nu}'(\bar{\mu}'(n' + f'(M')) = \bar{\nu}'(\mu'(n') + f(M)) = \nu'(\mu'(n')) + f''(M'') = 0$, since $Im(\mu') = ker(\nu')$. Thus, $Im(\bar{\mu}') \subseteq ker(\bar{\nu}')$.
  Next, $n+f(M) \in ker(\bar{\nu}') \implies \nu'(n) = f''(m'')$ for some $m'' \in M''$ similar to the previous. Now, since ν is surjective, $m'' = \nu(m)$ for some $m \in M$. Note that $\nu'(n - f(m)) = \nu'(n) - \nu'(f(m)) = f''(m'') - f''(\nu(m)) = f''(m'') - f''(m'') = 0 \implies n - f(m) \in ker(\nu') \implies n - f(m) \in Im(\mu') \implies \mu'(n') = n - f(m)$ for some $n' \in N'$. And so finally, $\bar{\mu}'(n' + f'(M')) = \mu(n') + f(M) = n - f(m) + f(M) = n + f(M) \implies n + f(M) \in Im(\bar{\mu}') \implies ker(\bar{\nu}') \subseteq Im(\bar{\mu}')$, and we are done.

- $\bar{\nu}'$ is surjective: Since ν' is surjective, $\forall n'' \exists n$ such that $\nu'(n) = n''$. Then, for each $n'' + f''(M'') \in Coker(f'')$, we have $\bar{\nu}'(n + f(M)) = n'' + f''(M'')$.

□

The snake lemma is one of the basic results of homological algebra. It is easy to see where it gets its name from from this expanded version of the diagram:



Definition. *Let C be a class of R-modules and $\lambda : C \to Z$ be a function. Then, λ is said to be additive if for each short exact sequence such as $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ in which each term belongs to $C, \lambda(M') - \lambda(M) + \lambda(M'') = 0$.*

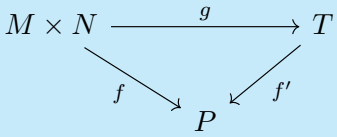
Example. Let C be the class of all finite-dimensional vector spaces V over a field F. Then, $f : V \to \dim V$ is an additive function on C (this can be seen by an easy application of the rank-nullity theorem).

Theorem 2.9. *Let $0 \to M_0 \to M_1 \to ... \to M_n \to 0$ be an exact sequence of R-modules in which all the modules M_i and the kernels of all the homomorphisms belong to a class C. Then, for any additive function λ on C, we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

Proof. Split up the sequence into short exact sequences $0 \to N_i \to M_i \to N_{i+1} \to 0$, where $N_i = Im(f_i), N_0 = N_{n+1} = 0$. Then, we have $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. Taking an alternating sum cancels out all the terms except $\lambda(N_0) + \lambda(N_{n+1}) = 2\lambda(0) = 0$. □

Definition. *The tensor product of two R-modules M, N is a pair (T, g) where $T = M \otimes_R N$ is an R-module and $g : M \times N \to T$ is an R-bilinear map such that, given any R-module P and bilinear map $f : M \times N \to P$, there exists a unique linear map $f' : T \to P$ such that the following diagram commutes:*



A tensor product helps us by allowing us to deal with the nicer linear maps in place of bilinear ones, since every bilinear function on $M \times N$ factors into a linear one through T.

Theorem 2.10. *The tensor product of any two modules exists and is unique upto isomorphism.*

Proof. 1. Uniqueness: Suppose (T_1, g_1) and (T_2, g_2) are both $M \otimes N$. Considering the first and replacing (P, f) with (T_2, g_2) gives us a unique linear map $j : T_1 \to T_2$ such that $g_2 = j \circ g_1$. Now, interchanging the roles of T_1 and T_2 gives us another unique linear map $j' : T_2 \to T_1$ such that $g_1 = j' \circ g_2$. Clearly, $j \circ j' = j' \circ j = Id \implies j$ is an isomorphism, and we are done.

2. Existence: Let C be the free R-module over $M \times N$. An arbitrary element in it is of the form $\sum_{i=1}^{n} r_i(x_i, y_i)$.
Next, let D be the submodule of C generated by all elements of the following types:

   - $(x + x', y) - (x, y) - (x', y)$
   - $(x, y + y') - (x, y) - (x, y')$
   - $(ax, y) - a(x, y)$
   - $(x, ay) - a(x, y)$.

   Finally, define $T = C/D$, and let $x \otimes y$ denote the image of $(x, y) \in C$ in T; T is generated by elements of the form $x \otimes y$.
   It is easy to check that the mapping $g : M \times N \to T, g(x, y) = x \otimes y$ is bilinear by construction. We claim that the pair (T, g) is the required tensor product.
   Any map $f : M \times N \to P$ can extend linearly to an R-module homomorphism $\bar{f} : C \to P$. If f happens to be bilinear in particular, then it vanishes on D and so induces a well-defined homomorphism $f' : T \to P$ such that $f'(x \otimes y) = f(x, y)$; since f' is uniquely defined by this condition, (T, g) satisfy the requirements of being a tensor product.

□

Remark. $\{x \otimes y\}$ generate T, where $x \in M, y \in N$.

Example. Let $R = \mathbb{Z}, M = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z} = M' \subseteq M, N' = N$. Let x be the nonzero element in N'. Then, as an element of $M \otimes N, 2 \otimes x = 1 \otimes 2x = 1 \otimes 0 = 0$.
On the other hand, suppose it is zero as an element of $M' \otimes N'$. Clearly, this would mean $M' \otimes N' = 0$. But this would also mean any map from $2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ to any R-module (in particular, $\mathbb{Z}/2\mathbb{Z}$) would be trivial, which is not true of (for example) $f(2z, x) = zx$.

Corollary 2.10.1. *Let $x_i \in M, y_i \in N$ such that $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Then there exist finitely generated submodules $M_0 \subseteq M, N_0 \subseteq N$, such that $x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.*

Proof. If $\sum x_i \otimes y_i = 0$ in $M \otimes N \implies \sum(x_i, y_i) = 0$ in $C/D \implies \sum(x_i, y_i)$ is a finite linear combination of the generators of D.
Let M_0 be generated by the x_i and the elements of M which occur as the first coordinates in those generators of D, and define N_0 similarly.
Therefore, by construction, $\sum(x_i, y_i) \in D'$, where D' is the analogously defined submodule of the free module over $M_0 \times N_0$; and so finally, $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$. □

Definition (Multitensor product)**.** *Let $M_1, ...M_r$ be modules. Their tensor product $M_1 \otimes ... \otimes M_r$ is another module T along with a multilinear map $g : M_1 \times ... \times M_r \to T$ such that for any R-module P and multilinear map $f : M_1 \times ... \times M_r \to P$, there exists a unique homomorphism $f : T' \to P$ such that $f' \circ g = f$.*

Theorem 2.11. *Let M, N, P be R-modules. Then, the following modules are isomorphic:*

1. $M \otimes N \cong N \otimes M$
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$
3. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$
4. $R \otimes M \cong M$

Proof. We shall construct certain canonical isomorphisms between the enumerated modules.

1. Consider the mapping $(x, y) \mapsto y \otimes x$ from $M \times N \to N \otimes M$. Since this is bilinear, it induces a homomorphism $f : M \otimes N \to N \otimes M$ such that $f(x \otimes y) = y \otimes x$.
   We can analogously construct a homomorphism $g : N \otimes M \to M \otimes N, g(y \otimes x) = x \otimes y$.
   Since $f \circ g$ and $g \circ f$ are identity maps, they are each isomorphisms, and so $M \otimes N \cong N \otimes M$.

2. We shall first construct homomorphisms $f, g : (M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$. and show that they are well-defined.
   First, fix $z \in P$ and consider the map $(x, y) \mapsto x \otimes y \otimes z$ from $M \times N \to P'$. This is bilinear and thus induces a homomorphism $f_z : M \otimes N \to P' = M \otimes N \otimes P$ such that $f_z(\tau(x, y)) = f_z(x \otimes y) = x \otimes y \otimes z$.
   Next, consider the mapping $(t, z) \mapsto f_z(t)$ from $(M \otimes N) \times P \to M \otimes N \otimes P$. This is bilinear; similarly, it induces a homomorphism $f : (M \otimes N) \otimes P \to M \otimes N \otimes P$ such that $f((x \otimes y) \otimes z) = x \otimes y \otimes z$.
   Next, consider the map $(x, y, z) \mapsto (x \otimes y) \otimes z$ from $M \times N \times P \to (M \otimes N) \otimes P$. Since this is linear in each variable, it induces a homomorphism $g : M \otimes N \otimes P \to (M \otimes N) \otimes P, g(x \otimes y \otimes z) = (x \otimes y) \otimes z$.
   To see that they are isomorphisms, note that $f \circ g$ and $g \circ f$ are identity maps. Thus, $(M \otimes N) \otimes P \cong M \otimes N \otimes P$.
   A similar construction will work to show that $M \otimes (N \otimes P) \cong M \otimes N \otimes P$.

3. Consider the mapping $((x, y), z) \mapsto (x \otimes z, y \otimes z)$ from $(M \oplus N) \times P \to (M \otimes P) \oplus (N \otimes P)$. Being bilinear (this can be verified easily), it induces a homomorphism $f' : (M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P), f'((x, y) \otimes z) = (x \otimes z, y \otimes z)$.

On the other hand, consider the bilinear maps $j_1 : M \times P \to (M \oplus N) \otimes P$ such that $j_1(x, z) = (x, 0) \otimes z$, and $j_2 : N \times P \to (M \oplus N) \otimes P$ such that $j_2(y, z) = (0, y) \otimes z$. These both induce homomorphisms $\bar{j_1}(x \otimes z) = (x, 0) \otimes z$ and $\bar{j_2}(y \otimes z) = (0, y) \otimes z$.

Finally, consider the homomorphism $j : (M \otimes P) \oplus (N \otimes P) \to (M \oplus N) \otimes P$, such that $j(x \otimes z, y \otimes z) = \bar{j_1}(x \otimes z) + \bar{j_2}(y \otimes z) = (x, 0) \otimes z + (0, y) \otimes z = (x, y) \otimes z$.

Clearly, $f \circ j$ and $j \circ f$ are the identity mappings; therefore, f is an isomorphism. We conclude that $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$.

4. Consider the canonical mapping $(r, m) \to rm$ from $R \times M \to M$. Since this is bilinear, it induces a homomorphism $f : R \otimes M \to M$ such that $f(r \otimes m) = rm$.
On the other hand, consider $g : M \to R \otimes M$ such that $g(x) = 1 \otimes x$. $g \circ f(a \otimes x) = g(ax) = 1 \otimes ax = a \otimes x \implies g \circ f = Id$. Similarly, $f \circ g(1 \otimes x) = f(x) = f(1x) = 1 \otimes x \implies f \circ g = Id$.
Thus, f is an isomorphism $\implies R \otimes M \cong M$.

□

Remark. The third part of the above theorem states, in effect, that the tensor product distributes over the direct sum.

Lemma 2.12. $Hom(M \otimes N, P) \cong Hom(M, Hom(N, P))$

Proof. Let $f : M \times N \to P$ be a bilinear map. This induces a linear map $f_x : N \to P, f_x(y) = f(x, y)$. Thus, f induces a map from $M \to Hom(N, P), x \mapsto f_x$. This will also be linear, since f is linear in x.
Conversely, consider any homomorphism $\phi : M \to Hom(N, P)$. This will define a bilinear map from $M \times N \to P, (x, y) \mapsto (\phi(x)) \circ (y)$.
Thus, the set S of bilinear mappings $M \times N \to P$ is in one-one correspondence with $Hom(M, Hom(N, P))$.
On the other hand, S is naturally in one-one correspondence with $Hom(M \otimes N, P)$ by the defining property of the tensor product. Hence, proved. □

Definition. *Let $f : M \to M', g : N \to N'$ be two module homomorphisms and define $h : M \times N \to M' \otimes N', h(x, y) = f(x) \otimes g(y)$. It is easy to see that h is bilinear. Thus, it induces a homomorphism $f \otimes g : M \otimes N \to M' \otimes N'$ such that $(f \otimes g(\tau(x, y)) = h(x, y) \iff (f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.*

Theorem 2.13. *Let*

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

be an exact sequence, and let N be any module. Then,

$$M' \otimes N \xrightarrow{f \otimes Id_N} M \otimes N \xrightarrow{g \otimes Id_N} M'' \otimes N \to 0$$

is exact.

Proof. Let P be a module. By theorem 2.7, the sequence

$$0 \to Hom(M'', Hom(N, P)) \xrightarrow{\bar{g}} Hom(M, Hom(N, P)) \xrightarrow{\bar{f}} Hom(M', Hom(N, P))$$

is exact.
By lemma 2.12, the sequence

$$0 \to Hom(M'' \otimes N, P) \xrightarrow{\bar{g}'} Hom(M \otimes N, P) \xrightarrow{\bar{f}'} Hom(M' \otimes N, P)$$

is exact.
And so by another application of theorem 2.7, we conclude that the sequence

$$M' \otimes N \xrightarrow{f \otimes Id_N} M \otimes N \xrightarrow{g \otimes Id_N} M'' \otimes N \to 0$$

is exact. It remains to be seen why the maps are of the stated form. Consider $\bar{f}'$. This is obtained by a composition of the maps $Hom(M \otimes N, P) \to Hom(M, Hom(N, P)) \xrightarrow{-\circ f} Hom(M', Hom(N, P)) \to Hom(M' \otimes N, P)$. The last isomorphism is given by $\alpha(\phi)(m \otimes n) = \phi(m)(n) = h_m(n)$, where $\phi : M' \to Hom(N, P), h_m : N \to P$.
Thus, the maps composed are $((m \otimes n) \mapsto h_m(n)) \to (m \mapsto h_m) \to (m' \mapsto h_{f(m')}) \to (m' \otimes n \mapsto h_{f(m')}(n))$. Overall, the map amounts to precomposition with $f \otimes Id_N$. □

Example. Let $R = \mathbb{Z}$, and consider an exact sequence $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$, where $f(x) = 2x$.
Tensor this sequence with $N = \mathbb{Z}/2\mathbb{Z}$. The sequence $0 \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes 1} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ is not exact, because $(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0 \implies f \otimes 1 = 0$, but $\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \neq 0$.
This shows that the last zero term in the statement of theorem 2.13 is crucial for it to hold.

Remark. If we define $T(M) = M \otimes N, U(P) = Hom(N, P)$, then lemma 2.12 states that, for all modules M, P, $\mathrm{Hom}(T(M), P) \cong \mathrm{Hom}(M, U(P))$.
In category-theoretic terms, the functor T is the left-adjoint of U, and U is the right-adjoint of T; and the above theorem states that any functor which is a left adjoint is right exact (where the 'right' signifies the necessity of a 0 at the right end). As it so turns out, it is also true that any functor which is a right adjoint is left exact.

Definition. *If tensoring with N transforms all exact sequenes into exact sequences, then N is said to be a flat R-module.*

Theorem 2.14. *The following are equivalent for an R-module N:*

1. *N is flat*
2. *If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact*
3. *If $f : M' \to M$ is injective, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.*
4. *If $f : M' \to M$ is injective and M, M' are finitely generated, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.*

Proof. 4 $\implies$ 3: Suppose $f : M' \to M$ is injective and let $u = \sum x'_i \otimes y_i \in ker(f \otimes 1) \subseteq M' \otimes N \implies \sum f(x'_i) \otimes y_i = 0 \in M \otimes N$. We wish to show that $u = 0$.
By corollary 2.10.1, there exist finitely generated submodules $M_0 \subseteq M, N_0 \subseteq N$, such that $\sum f(x'_i) \otimes y_i = 0 \in M_0 \otimes N_0$.

Let $M_0' \subseteq M'$ be generated by $\{x_i'\}$, and $u_0 = \sum x_i' \otimes y_i$ be the corresponding element in $M_0' \otimes N_0$. Then, for the restriction $f_0 : M_0' \to M_0, (f_0 \otimes 1)(u_0) = 0 \implies u_0 = 0 \in M_0' \otimes N_0$, since $f_0 \otimes 1$ is injective by assumption (M_0, M_0' are finitely generated). Thus, $u = 0 \in M \otimes N$, and we are done.

$1 \implies 2$ is trivial from definition, but $2 \implies 1$ is *not*; it tells us that if a module preserves short exact sequences on tensoring, it must preserve long exact sequences as well. It can be proven by breaking up an LES into SES and applying flatness on each.

$2 \implies 3, 3 \implies 4$ are trivial. 3, together with theorem 2.13, implies 2. □

Definition. *Let $f : A \to B$ be a ring homomorphism and M, N be modules over A, B respectively. Then:*

1. *N has an A-module structure by restriction of scalars as follows: If $a \in A, x \in N$, then $(a, x) \to f(a)x$.*
2. *In this way, B can also be regarded as an A-module; and so the tensor product $M_B = B \otimes M$ is an A-module. This can be given B-module structure by extension of scalars as follows: If $b \in B, b' \otimes x \in M_B$, then $(b', b \otimes x) \to bb' \otimes x$. M_B is an (A, B)-bimodule.*
3. *The ring B, equipped with the A-module structure (via the homomorphism), is said to be an A-algebra. An A-algebra is a ring B and a homomorphism $f : A \to B$.*
4. *An A-algebra homomorphism $h : B \to C$ is a ring homomorphism which is also a module homomorphism.*

- An A-algebra B and the associated ring homomorphism $f : A \to B$ are *finite* if B is finitely generated as an A-module.
- The homomorphism is of *finite type*, and B is a *finitely generated A-algebra*, if there exists a finite set of elements in B, $\{x_1, , ., x_n\}$ such that every element of B can be written as a polynomial in them with coefficients in $f(A)$. Note that this is weaker than saying they are finite.
- A ring A is said to be finitely generated if it is finitely generated as a $\mathbb{Z}-$algebra.

Remark. Two remarks can be made here.

1. Every ring is a $\mathbb{Z}$-algebra by virtue of the natural homomorphism $f : \mathbb{Z} \to A, f(n) = n.1$.
2. If R is a field, an R-algebra is effectively a ring containing R as a subring (since any homomorphism $f : R \to S$ will be injective).

Theorem 2.15. *The following statements hold for modules obtained via restriction & extension of scalars:*

1. *Suppose N is finitely generated as a B-module and B is finitely generated as an A-module. Then N is finitely generated as an A-module.*
2. *If M is finitely generated as an A-module, M_B is finitely generated as a B-module.*

Proof. 1. If $\{y_i\}_{i=1}^n$ generates N over B and $\{x_i\}_{i=1}^n$ generates B over A, then the mn products $x_i y_i$ generates N over A.

2. If $\{x_i\}_{i=1}^n$ generates M over A, then $\{1 \otimes x_i\}_{i=1}^n$ generates M_B over B.

□

Corollary 2.15.1. *M is a flat A-module $\implies$ M_B is a flat B-module.*

Proof. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of B-modules. Then:
$0 \to M' \otimes_B M_B \to M \otimes_B M_B \to M'' \otimes_B M_B \to 0$
$\equiv 0 \to M' \otimes_B (B \otimes_A M) \to M \otimes_B (B \otimes_A M) \to M'' \otimes_B (B \otimes_A M) \to 0$
$\equiv 0 \to (M' \otimes_B B) \otimes_A M \to (M \otimes_B B) \otimes_A M \to (M'' \otimes_B B) \otimes_A M \to 0$, which is an exact sequence of A-modules by flatness of M. By an application of theorem 2.14, we conclude that M_B is flat as a B-module.

Note that here we have used the fact that for an A-module M, B-module P, and (A, B)-bimodule N, $(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$. This can be proven in the following manner:
The map $f_z(x, y) = x \otimes_A (y \otimes_B z)$ is bilinear and thus yields a homomorphism $M \otimes_A N \to M \otimes_A (N \otimes_B P)$. Next, the map $g(x \otimes_A y, z) = x \otimes_A (y \otimes_B z)$ is bilinear and thus yields a homomorphism $(M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$. A symmetric argument will construct its inverse and show that the two are isomorphisms. □

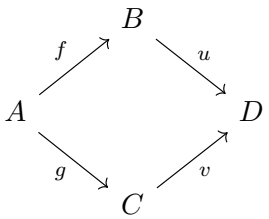
Lemma 2.16. *Let $f : A \to B, g : A \to C, h : B \to C$ be ring homomorphisms. Then h is an A-algebra homomorphism if and only if $h \circ f = g$.*

Proof. If $h \circ f = g$, then $h(ax) = h(f(a)x) = h(f(a))h(x) = g(a)h(x) = ah(x)$, and we are done. Conversely, if h is a module homomorphism, then $h(ax) = ah(x) \iff h(f(a))h(x) = g(a)h(x) \forall x \iff h \circ f = g$. □

Example. We shall turn $D = B \otimes_A C$ into an A-algebra (where B and C are A-algebras with homomorphisms f and g respectively).

First, we need to define a multiplication on D.
Consider the mapping $B \times C \times B \times C \to D$ defined by $(b, c, b', c') \mapsto bb' \otimes cc'$. This is multilinear and so induces a homomorphism $B \otimes C \otimes B \otimes C \to D$. By theorem 2.24, this will be a homomorphism from $D \otimes D \to D$.
This homomorphism will, in turn, correspond to a bilinear map $\mu : D \times D \to D$ such that $\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'$.
With this multiplication, D becomes a commutative ring with identity $1 \otimes 1$. Finally, with the homomorphism $a \mapsto f(a) \otimes g(a), D$ procures the A-algebra structure.

Remark. The following diagram commutes:



where $u(b) = b \otimes 1, v(c) = 1 \otimes c$. This is because $f(a) \otimes 1 = (f(a).1) \otimes 1 = (a.1) \otimes 1 = a(1 \otimes 1) = 1 \otimes (a.1) = 1 \otimes g(a) \in B \otimes C = D$.

Exercises

Direct limits:

A direct limit is a way to construct a large object from smaller ones in a certain way. It is a special case of the concept of a *colimit* in category theory. We shall construct the direct limit of a collection of modules.

A partially ordered set I is called a *directed set* if for every pair of elements $i, j \in I, \exists k \in I$ such that $i \leq k, j \leq k$.

Let R be a ring, I be a directed set and $(M_i)_{i \in I}$ be a family of modules over R. Further, for each pair $i, j \in I$ such that $i \leq j$, let $\mu_{ij} : M_i \to M_j$ be a homomorphism and suppose the following conditions are satisfied:

1. μ_{ii} is the identity mapping of $M_i, \forall i \in I$
2. $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ whenever $i \leq j \leq k$.

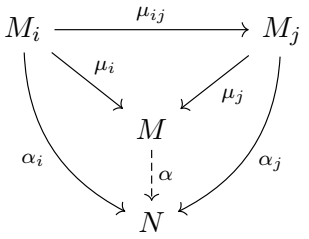
Then, $\mathbf{M}$=(M_i, μ_{ij}) are said to form a *direct system* over I.

Finally, we shall construct a module M which will be known as the *direct limit* of the direct system $\mathbf{M}$. Let $C = \bigoplus_{i \in I} M_i$, and $\phi_i : M_i \to M$ be the natural injection map. Define a submodule $D \subseteq C$ as being generated by all elements of the form $(\phi_i - \phi_j \circ \mu_{ij})(x_i)$, where $i \leq j$.

Let $M = C/D$, and $\mu : C \to M$ be the natural quotient map. Let μ_i be its restriction to M_i, that is, $\mu_i(x_i) = \phi_i(x_i) + D$. Clearly, $\mu_i(x_i) = \phi_i(x_i) + D = \phi_j \circ \mu_{ij}(x_i) + D = \mu_j \circ \mu_{ij}(x_i) \iff \mu_i = \mu_j \circ \mu_{ij}, i \leq j$. The pair $(M, \{\mu_i\}_{i \in I})$ is called the *direct limit* of the direct system $\mathbf{M}$ and is represented by $\varinjlim M_i$.

An alternative helpful way of characterizing direct limits is as follows: Given a direct system (M_i, μ_{ij}), for any module N, consider homomorphisms $\alpha_i : M_i \to N$ such that $\alpha_i = \alpha_j \circ \mu_{ij}$ whenever $i \leq j$. The direct limit of the system is a module M such that there exists a unique homomorphism from $M \to N$ which satisfies $\alpha_i = \alpha \circ \mu_i$.

In other words, it is the pair $(M, \{\mu_i\}_{i \in I})$ which makes the following diagram commute uniquely for every $(N, \{\alpha_i\}_{i \in I})$:



It is a special one of all the possible pairs $(N, \{\alpha_i\}_{i \in I})$; if we call each pair a *target*, the direct limit is the *universally repelling target.*

Discussion. The notion of a direct limit satisfies a number of nice properties.

- Any module is the direct limit of its finitely generated submodules:

  Let $(M_i)_{i\in I}$ be a family of submodules of some $R-$module such that for any pair $i, j \in I, \exists k \in I$ such that $M_i + M_j \subseteq M_k$. Define $i \leq j \equiv M_i \subseteq M_j$. It is clear that, under this order, I is a directed set. If we define $\mu_{ij} : M_i \to M_j$ to be the embedding of M_i in M_j, then (M_i, μ_{ij}) form a direct system.

  We need to show that $\varinjlim M_i = \bigcup M_i$. Given this, let M be a module and $(M_x)_{x\in M}$ be a family of submodules, where M_x is the submodule generated by x. Any two finitely generated submodules M_x, M_y are contained in a third finitely generated submodule, $M_x + M_y$. Therefore, $M = \bigcup M_x = \varinjlim M_x$, and the statement follows.

- Direct limits preserve exactness:

  Let $\mathbf{M}$=(M_i, μ_{ij}), $\mathbf{N}$=(N_i, ν_{ij}), $\mathbf{P}$=(P_i, η_{ij}) be three direct systems over the same directed set I, and M, N, P be their direct limits with families of homomorphisms μ_i, ν_i, η_i.

  The homomorphism $\Phi : \mathbf{M} \to \mathbf{N}$ is defined by a family of homomorphisms $\phi_i : M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$. It can be shown that this defines a unique homomorphism $\phi = \varinjlim \phi_i : M \to N$ such that $\phi \circ \mu_i = \nu_i \circ \phi_i$.

  Let $\Theta : \mathbf{N} \to \mathbf{P}, \theta_i : N_i \to P_i, \theta : N \to P$ be defined analogously. Then, the following holds:

  If $M_i \xrightarrow{\phi_i} N_i \xrightarrow{\theta_i} P_i$ is exact $\forall i \in I$, then $M \xrightarrow{\phi} N \xrightarrow{\theta} P$ is exact. Another way of stating the precondition is to say that the sequence $\mathbf{M} \xrightarrow{\Phi} \mathbf{N} \xrightarrow{\Theta} \mathbf{P}$ is exact.

- Tensor products commute with direct limits:

  Let (M_i, μ_{ij}) form a directed system over I. It is clear that for any module N, $(M_i \otimes N, \mu_{ij} \otimes 1)$ forms a direct system. Then, the following holds:

  $\varinjlim (M_i \otimes N) \cong (\varinjlim M_i) \otimes N$.

Ring of fractions

Definition. *The field of fractions of an integral domain R is $R \times (R/\{0\})/\sim$, where $\sim$ is an equivalence relation on $R \times (R/\{0\})$ defined by $(a,s) \sim (b,t) \iff at - bs = 0$.*

Lemma 3.1. *$\sim$ is an equivalence relation.*

Proof. It is obvious that it is reflexive. Further, $(a,s) \sim (b,t) \iff at - bs = 0 \iff bs - at = 0 \iff (b,t) \sim (a,s) \implies$ it is symmetric.
Finally, suppose $(a,b) \sim (c,d) \implies ad = bc$, and $(c,d) \sim (e,f) \implies cf = de$. Then, $adf = bcf, bde = bcf \implies adf = bde \implies af = be$ (since R is an integral domain) $\implies (a,b) \sim (e,f)$. Thus, $\sim$ is transitive as well. □

We shall generalize this construction to rings which are not integral domains.

Discussion. Let R be any ring and S be a multiplicatively closed subset of R, i.e., $1 \in S$ and S is closed under multiplication, i.e., S is a sub-semigroup of $(R, \cdot)$. Define $\equiv$ on $R \times S : (a,s) \equiv (b,t) \iff (at - bs)u = 0$ for some $u \in S$.
It is clear that this relation is symmetric. Furthermore, since $1 \in S$, it is also reflexive. To show that it is transitive, suppose $(a,s) \equiv (b,t) \implies atv = bsv$ for some $v \in S$ and $(b,t) \equiv (c,u) \implies buw = ctw, w \in S$. We then have $au(tvw) = (buw)sv = cs(tvw) \implies (au - cs)tvw = 0$. Since S is closed under multiplication, $tvw \in S \implies (a,s) \equiv (c,u)$. Therefore, $\equiv$ is transitive, and we conclude that it is an equivalence relation.
Denote $[(a,s)]$ by $\frac{a}{s}$ and $R \times S/\equiv$ by $S^{-1}R$, and define the following operations:

- $+ : S^{-1}R \times S^{-1}R \to S^{-1}R, (\frac{a}{s} + \frac{b}{t}) = \frac{(at +_R bs)}{st}$
- $\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R, \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$.

Then, $(S^{-1}R, +, \cdot)$ is the *ring of fractions* of R with respect to S. It will also satisfy a *universal property*, stated in theorem 3.32.

Remark. If R is an integral domain and $S = R/\{0\}$, then $S^{-1}R$ is a field (the field of fractions).

Lemma 3.2. *$(S^{-1}R, +, \cdot)$ is a commutative ring with identity.*

Proof. First, we must show that $+, \cdot$ are well-defined. It suffices to show that $(a_1, s_1) \equiv (a_2, s_2) \implies \frac{a_1}{s_1} + \frac{b}{t} = \frac{a_2}{s_2} + \frac{b}{t}; \frac{a_1 b}{s_1 t} = \frac{a_2 b}{s_2 t}$. This is easy to check.
Commutativity of the operations follows from commutativity of R. Additive identity, additive inverse and multiplicative identity are $\frac{0}{s}, \frac{-a}{s}$ and $\frac{1}{1}$ respectively. Associativity and distributivity of the operations follows from the same in R. □

Theorem 3.3. *Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in $B, \forall s \in S$; and let $f : A \to S^{-1}A$ be the homomorphism $f(x) = \frac{x}{1}$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.*

Proof. We need to prove the existence and uniqueness of h.

1. Uniqueness: Suppose h satisfies the given conditions. Then, $h(\frac{a}{1}) = hf(a) = g(a), \forall a \in A$.
   If $s \in S, h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s)^{-1}$.
   Therefore, $h(\frac{a}{s}) = g(a)g(s)^{-1}$, and h is uniquely determined by g.

2. Existence: Define $h(\frac{a}{s}) = g(a)g(s)^{-1}$. First, we show that h is well-defined.
   $\frac{a}{s} = \frac{a'}{s'} \implies (as' - a's)t = 0, t \in S \implies (g(a)g(s') - g(a')g(s))g(t) = 0 \implies g(a)g(s') = g(a')g(s)$, multiplying both sides by $g(t)^{-1}$. Hence, $g(a)g(s)^{-1} = g(a')g(s')^{-1} \implies h(\frac{a}{s}) = h(\frac{a'}{s'})$.
   $h(\frac{a}{s} + \frac{a'}{s'}) = h(\frac{as'+a's}{ss'}) = g(as' + a's)g(ss')^{-1} = g(a)g(s)^{-1} + g(a')g(s')^{-1} = h(\frac{a}{s}) + h(\frac{a'}{s'}); h(\frac{a'}{s'}\frac{a}{s}) = g(aa')g(ss')^{-1} = g(a)g(s)^{-1}g(a')g(s')^{-1} = h(\frac{a'}{s'})h(\frac{a}{s}) \implies h$ is a homomorphism on $S^{-1}A$.

□

Remark. The function f is not, in general, injective, since we could always have, for $x \neq y, (x - y)u = 0$ for $u \in S \implies f(x) = f(y)$.

Corollary 3.3.1. *If $g : A \to B$ is a ring homomorphism such that*

1. *$s \in S \implies g(s)$ is a unit in B*
2. *$g(a) = 0 \implies as = 0$ for some $s \in S$*
3. *Every element in B is of the form $g(a)g(s)^{-1}$,*

then there exists a unique isomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.

Proof. We have to show that $h(\frac{a}{s}) := g(a)g(s)^{-1}$ is an isomorphism. By (3), it is surjective. But also, $h(\frac{a}{s}) = 0 \implies g(a) = 0 \implies at = 0, t \in S \implies \frac{a}{s} \sim \frac{0}{t} \implies \frac{a}{s} = 0 \implies h$ is injective, and we are done. □

Remark. In particular, it is easy to see that the ring $S^{-1}A$ and f also satisfy these properties, in which case the isomorphism h is merely identity.

Discussion. For any multiplicatively closed set with 1 S, the above construction of $S^{-1}A$ can be reproduced for any $A-$module M to construct $S^{-1}M$ by defining $\equiv$ on $M \times S$ as $(m, s) \equiv (m's') \iff \exists t \in S : t(sm' - ms') = 0$. Verification of the fact that $\equiv$ is an equivalence relation remains unchanged. If $\frac{m}{s}$ denotes the equivalence class of (m, s) and $S^{-1}M = M \times S/\equiv$, we can turn $S^{-1}M$ into an $S^{-1}A-$module with the obvious addition and multiplication.

If $u : M \to N$ is an $A-$module homomorphism, there is a natural $S^{-1}A-$module homomorphism $S^{-1}u : S^{-1}M \to S^{-1}N$ which maps $\frac{m}{s} \mapsto \frac{u(m)}{s}$. It is easy to see that $S^{-1}(\nu \circ \mu) = S^{-1}(\nu) \circ S^{-1}(\mu)$.

Example. $S = A/P$ is multiplicatively closed $\iff$ P is prime: $xy \notin A/P, x, y \in A/P \implies xy \in P, x, y \notin P$, which contradicts P being prime. On the other hand, $(x, y \in A/P \implies xy \in A/P) \iff (xy \in P \implies x \in P \text{ or } y \in P)$, so that P is prime. In this case, denote the ring of fractions $S^{-1}A$ by A_P.
We show that A_P is a local ring, and its maximal ideal M is given by $\{\frac{a}{s} : a \in P\}$.
It is easy to see that this is an ideal in A_P, by virtue of the fact that P is an ideal. On the other hand, $\frac{b}{t} \notin M \implies b \notin P \implies b \in S \implies \frac{t}{b} \in A_P \implies \frac{b}{t}$ is a unit; so that for any ideal $I, I \not\subset M \implies I = R$ (since I will have a unit). The uniqueness of M follows from the fact that it contains every non-unit in A_P.
As an example of this, consider $A = \mathbb{Z}$ and $P = (p)$ for some prime p. Then $A_P = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \notin P\}$.

The process of passing from A to A_P is called *localization* at P. It is the algebraic analogue of the geometric notion of concentrating attention near a point.

We can also take S to be the set of all non-zero-divisors in R. It is easy to see that this will be multiplicatively closed; furthermore, the natural homomorphism $r \mapsto \frac{r}{1}$ will be injective. In this case, the action of S^{-1} is to turn all non-zero-divisors into *units* by supplying them with inverses in the ring of fractions (for a non-zero-divisor s, its inverse in the ring of fractions will be $\frac{1}{s}$). It is easy to see that in the localization of A to A_P, what we have done is added inverses to all elements not in P. We are 'zooming in' on P by getting rid of obstructions from other points.

As another example, let $A = k[t_1, ...t_n]$, where k is a field and $\{t_i\}$ are indeterminates. If P is a prime ideal in A, then $A_P = \{\frac{f}{g} : f, g \in A, g \notin P\}$, similar to the previous case, and let V be the variety defined by P, $V = \{x = (x_1, ...x_n) \in k^n : f(x) = 0, \forall f \in P\}$.
Once again, what we have done with localization is supplied inverses to elements not in P. Now, $g \notin P \implies g \neq 0$ almost everywhere on V, because $I(V(P)) = \sqrt{P} = P$ (the first equality is Hilbert's Nullstellensatz, and the second one is because P is prime).
Thus, A_P can be identified with the ring of all rational functions on k^n which are defined at almost all points of V. A_P is the *local ring of k^n along the variety V*, and is the 'prototype of the local rings which arise in algebraic geometry.'

Theorem 3.4. *If $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact at M, $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ is exact at $S^{-1}M$. In other words, the operation S^{-1} is exact.*

Proof. $g \circ f = 0 \implies S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = S^{-1}(0) = 0 \implies Im(S^{-1}f) \subseteq Ker(S^{-1}g)$. On the other hand, let $\frac{m}{s} \in ker(S^{-1}g) \implies \frac{g(m)}{s} = 0 \in S^{-1}M'' \implies \exists t \in S$ such that $g(tm) = tg(m) = 0 \in M'' \implies tm \in ker(g) \implies tm = f(m'), m' \in M' \implies \frac{m}{s} = \frac{f(m')}{ts} = S^{-1}(f)(\frac{m'}{st}) \implies \frac{m}{s} \in Im(S^{-1}f) \implies ker(S^{-1}g) \subseteq Im(S^{-1}f)$, and we are done. □

Corollary 3.4.1. *For submodules N, P of M:*

1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$
3. $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$

Proof. We prove each statement in turn.

1. $S^{-1}(N+P) = \{\frac{n+p}{s} : n \in N, p \in P\} = \{\frac{n}{s} + \frac{p}{s} : n \in N, p \in P\} = S^{-1}(N) + S^{-1}(P)$
2. For $y \in N, z \in P, s, t \in S$, let $\frac{y}{s} = \frac{z}{t} \in S^{-1}(N) \cap S^{-1}(P) \implies u(ty - sz) = 0, u \in S \implies w = uty = usz \in N \cap P \implies \frac{y}{s} = \frac{w}{sty} \in S^{-1}(N \cap P) \implies S^{-1}(N) \cap S^{-1}(P) \subseteq S^{-1}(N \cap P)$. Conversely, $\frac{y}{s} \in S^{-1}(N \cap P) \implies y \in N \cap P \implies \frac{y}{s} \in S^{-1}(N), \frac{y}{s} \in S^{-1}(P) \implies \frac{y}{s} \in S^{-1}(N) \cap S^{-1}(P) \implies S^{-1}(N \cap P) \subseteq S^{-1}(N) \cap S^{-1}(P)$, and we are done.
3. Apply S^{-1} to the sequence $0 \to N \to M \to M/N \to 0$. Since $S^{-1}M \to S^{-1}M/N$ is surjective and its kernel equals the image of $S^{-1}N$ (which itself is isomorphic to $S^{-1}N$, since the first function is injective), the result follows from the first isomorphism theorem.

□

Remark. The above results tell us that the operation S^{-1} on modules is exact, and commutes with the formation of finite sums, finite intersections, and quotients.

Theorem 3.5. *There exists a unique isomorphism between $S^{-1}A$ modules $f : S^{-1}A \otimes_A M \to S^{-1}M, f((\frac{a}{s}) \otimes m) = \frac{am}{s}, \forall a \in A, m \in M, s \in S$.*

Proof. First, note that $S^{-1}A$ can be given $A-$module structure in the obvious manner, by restriction of scalars. Furthermore, by defining $\frac{a'}{s'}(\frac{a}{s} \otimes m) = (\frac{aa'}{ss'} \otimes m)$, i.e., by extension of scalars, we can give $S^{-1}A \otimes_A M$ an $S^{-1}A$-module structure.
Consider the mapping $S^{-1}A \times M \to S^{-1}M, (\frac{a}{s}, m) \mapsto \frac{am}{s}$. Since this is A-bilinear, it induces a homomorphism $f : S^{-1}A \otimes M \to S^{-1}M$ which will satisfy $f((\frac{a}{s}) \otimes m) = \frac{am}{s}$.
It is clear that f is surjective, and its uniqueness follows from the universal property of the tensor product.
Let $\sum_i(\frac{a_i}{s_i} \otimes m_i)$ be an arbitrary element of $S^{-1}A \otimes M$. Let $s = \Pi_i s_i \in S, t_i = \Pi_{i \neq j} s_i \in S$. Then, $\sum_i(\frac{a_i}{s_i} \otimes m_i) = \sum_i(\frac{a_i t_i}{s} \otimes m_i) = \frac{1}{s} \otimes \sum_i a_i t_i m_i \implies$ every element in $S^{-1}A \otimes M$ is of the form $\frac{1}{s} \otimes m$. Now, $f(\frac{1}{s} \otimes m) = 0 \implies \frac{m}{s} = 0 \implies tm = 0, t \in S \implies \frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0 \implies ker(f) = 0 \implies f$ is injective, and we are done. □

Corollary 3.5.1. *$S^{-1}A$ is a flat A-module.*

Proof. Suppose $0 \to M' \to M \to M'' \to 0$ is exact. Consider $0 \to S^{-1}A \otimes M' \to S^{-1}A \otimes M \to S^{-1}A \otimes M'' \to 0$. By 3.5, this is exact $\iff 0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$ is exact. But this is exact by 3.4. Thus, the tensored sequence is exact, and we conclude from theorem 2.14 that $S^{-1}A$ is flat. □

Corollary 3.5.2. *There exists a unique isomorphism between $S^{-1}A$ modules $f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N), f(\frac{m}{s} \otimes \frac{n}{t}) = \frac{(m \otimes n)}{st}$.*
In particular, if P is a prime ideal, then $M_P \otimes_{A_P} N_P \cong (M \otimes_A N)_P$ as A_P-modules.

Proof. $S^{-1}A \otimes_A M \cong S^{-1}M \iff S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} S^{-1}N$. But from the previous chapter, $(S^{-1}A \otimes_A M) \otimes_{S^{-1}A} S^{-1}N \cong M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}N) \cong M \otimes_A S^{-1}N = M \otimes_A (S^{-1}A \otimes_A N) \cong S^{-1}A \otimes_A (M \otimes_A N) \cong S^{-1}(M \otimes_A N)$, and we are done. □

Definition. *A property X of a ring or a module is said to be a local property if the following is true: A (or M) has $X \iff A_P$ (or M_P) has X for every prime ideal P of A.*

Following are some examples of local properties.

Theorem 3.6. *For an A-module M, $M = 0 \iff M_P = 0 \iff M_m = 0$ for all prime ideals P and maximal ideals m of A.*

Proof. We only need to show $M_m = 0 \forall m \implies M = 0$. Suppose that $M_m = 0 \forall m, M \neq 0$. Let $x \neq 0 \in M, I = Ann(x) \neq R$. Then, I is contained in some maximal ideal m. Now, $\frac{x}{1} = 0 \in M_m$ (since $M_m = 0$ by assumption). In other words, $ax = 0, a \in A - m$. This is a contradiction, since we had $Ann(x) \subseteq m$. We conclude that $M_m = 0$. □

Theorem 3.7. *Let $\phi : M \to N$ be an A-module homomorphism. Then, ϕ is injective (surjective) $\iff \phi_P : M_P \to N_P$ is injective (surjective) $\iff \phi_m : M_m \to N_m$ is injective (surjective) for all prime ideals P and maximal ideals m of A. Note that $\phi_P \equiv (A - P)^{-1}M(\phi)$.*

Proof. We prove each implication.

1. $1 \implies 2$: If ϕ is injective, $0 \to M \to N$ is exact $\iff 0 \to M_P \to N_P$ is exact $\iff \phi_P$ is injective. If ϕ is surjective, $M \to N \to 0$ is exact $\iff M_P \to N_P \to 0$ is exact $\iff \phi_P$ is surjective.

2. $2 \implies 3$ in both cases because every maximal ideal is prime.

3. $3 \implies 1$: Let $M' = Ker(\phi) \implies 0 \to M' \to M \to N$ is exact $\iff 0 \to M'_m \to M_m \to N_m$ is exact $\implies M'_m \cong Ker(\phi_m) = 0$ (since ϕ_m is injective) $\implies M' = 0$ (by the previous theorem) $\implies \phi$ is injective.
   On the other hand, if we let $N' = N/Im(\phi)$, then $M \to N \to N' \to 0$ is exact $\iff M_m \to N_m \to N'_m \to 0$ is exact $\implies N'_m = 0$ (since ϕ_m is surjective) $\implies N' = 0 \implies \phi$ is surjective.

□

Theorem 3.8. *Let M be an A-module. Then M is a flat A-module $\iff M_P$ is a flat A_P-module $\iff M_m$ is a flat A_m-module for all prime ideals P and maximal ideals m of A.*

Proof. We prove each implication.

1. M is flat $\implies A_P \otimes_A M$ is flat as an A_P-module (by corollary 2.15.1) $\implies M_P$ is flat (by theorem 3.5).

2. $2 \implies 3$ is obvious.

3. $\phi : N \to P$ is injective $\implies \phi_m : N_m \to P_m$ is injective (by theorem 3.7) $\implies \phi_m \otimes 1 : N_m \otimes_{A_m} M_m \to P_m \otimes_{A_m} M_m$ is injective (by theorem 2.14) $\implies \phi_m \otimes 1 : (N \otimes_A M)_m \to (P \otimes_A M)_m$ is injective (by corollary 3.5.2) $\implies \phi \otimes 1 : N \otimes_A M \to P \otimes_A M$ is injective (by theorem 3.5). Thus, by theorem 2.14, M is flat.

□

To conclude:

- Being the 0-module is a local property.
- Being injective/surjective is a local property.
- Being flat is a local property.

Theorem 3.9. *Let A be a ring, S be a multiplicatively closed subset of A, $f : A \to S^{-1}A$ be the natural homomorphism $f(a) = \frac{a}{1}$, C be the set of contracted ideals in A, and E be the set of extended ideals in $S^{-1}A$. I^e will be $S^{-1}I$ (considering I as a module on the right-hand side). The following holds:*

1. *Every ideal in $S^{-1}A$ is an extended ideal.*
2. *If I is an ideal in A, then $I^{ec} = \bigcup_{s\in S}(I : (s))$.*
3. *$I^e = S^{-1}A \iff I \cap S \neq \emptyset$.*
4. *$I \in C \iff$ no element of S is a zero divisor in A/I.*
5. *The prime ideals of $S^{-1}A$ are in one-one correspondence with the prime ideals of A which don't meet S (that is, which have empty intersection with S).*
6. *The operation S^{-1} on ideals commutes with the formation of radicals, (finite) products, sums and intersections.*

Proof.

1. Let $J \subseteq S^{-1}A$ be an ideal, and $\frac{x}{s} \in J \implies \frac{x}{1} \in J \implies x \in J^c \implies \frac{x}{s} \in J^{ce} \implies J \subseteq J^{ce}$. But we know, in any case, from theorem 1.13 that $J^{ce} \subseteq J$. Thus, $J = J^{ce} \implies J \in E$ by the same theorem, and we are done.

2. $x \in I^{ec} = (S^{-1}I)^c \iff \frac{x}{1} = \frac{a}{s}, a \in I, s \in S \iff (xs - a)t = 0, t \in S \iff xst \in I \iff x \in \bigcup_{s\in S}(I : (s)) \implies I^{ec} \subseteq \bigcup_{s\in S}(I : (s))$.
On the other hand, $x \in \bigcup_{s\in S}(I : (s)) \implies xs \in I \implies \frac{x}{1}\frac{s}{1} \in I^e \implies \frac{x}{1} \in I^e \implies x \in I^{ec}$, and we are done.

3. $I \cap S \neq \emptyset \implies s \in S \cap I \implies \frac{s}{1} \in I^e \implies \frac{s}{1}\frac{1}{s} = \frac{1}{1} \in I^e \implies I^e = S^{-1}A$.
On the other hand, $I^e = S^{-1}A \implies I^{ec} = \bigcup_{s\in S}(I : (s)) = (S^{-1}A)^c = A$. Therefore, $x \in A \implies x = ist, i \in I, s \in S, t \in A$. In particular, $x \in S \implies x = ist$ for some i, s, t. Then, $xs \in S, xs \in I \implies I \cap S \neq \emptyset$.

4. $I \in C \iff I^{ec} = I \iff (\exists s \in S : sx \in I \implies x \in I)$ (from (2)) $\iff s \in S$ is not a zero divisor in A/I for any s.

5. We know that if J is prime in $S^{-1}A$, then J^c is prime in A. On the other hand, suppose I is prime in A. Then, A/I is an integral domain. Let $\bar{S}$ be the image of S in A/I under the quotient map. Then from corollary 3.4.1, $(S^{-1}A/S^{-1}I) \cong \bar{S}^{-1}(A/I)$, which is also an integral domain if $I \cap S = \emptyset$ (since it will be contained in the field of fractions of A/I; if $I \cap S \neq \emptyset$, it will be the zero field); and so from theorem 1.3, $S^{-1}I$ is prime. This gives us the correspondence we need. (Observe that it does not make sense, here, to write $S^{-1}(A/I)$.)

6. For finite sums, it follows from the fact that, in general, $(I_1 + I_2)^e = Bf(I_1 + I_2) = Bf(I_1) + Bf(I_2) = I_1^e + I_2^e$.
   For finite products, it follows from the fact that, in general, $(I_1 I_2)^e = Bf(I_1 I_2) = Bf(I_1)Bf(I_2) = I_1^e I_2^e$.
   For finite intersections, it follows from corollary 3.14.
   For radical formation: $x \in r(I)^e \implies x = \sum_i b_i f(x_i)$. For some high enough power $n, x^n = \sum_i b_i' f(x_i^n)$ where each $x_i^n \in I \implies x^n \in I^e \implies x \in r(I^e) \implies r(I)^e \subseteq r(I^e)$, so that $S^{-1}r(I) \subseteq r(S^{-1}I)$.
   On the other hand, suppose $\frac{x}{s} \in r(S^{-1}I) \implies \frac{x^n}{s^n} \in S^{-1}I \implies \frac{x^n}{s^n} = \frac{a}{t}$ for some $a \in I, t \in S$. Therefore, $utx^n = uas^n$ for some $u \in S$. Multiplying both sides by $(ut)^{n-1}$, we can conclude that $(utx)^n \in I \implies utx \in r(I)$. Also, $uts \in S$. Therefore, $\frac{utx}{uts} = \frac{x}{s} \in S^{-1}r(I) \implies r(S^{-1}I) \subseteq S^{-1}r(I)$, and we are done.

□

Remark. Recall that in the proof of theorem 1.7, we had to show that if $x \in A$ is not nilpotent, there exists a prime ideal which does not contain x. There is a much swifter argument we can employ with our new tools.
Consider $S = (x^n)_{n \geq 0}$. By assumption, $0 \notin S \implies S^{-1}A = A_f \neq 0$. By theorem 1.4, A_f has a maximal ideal, whose contraction in A will be a prime ideal P which does not meet S (by the above theorem); so that $x \notin P$.

Corollary 3.9.1. *If N is the nilradical of A, then $S^{-1}N$ is the nilradical of $S^{-1}A$.*

Proof. Follows from theorem 3.9 (5) in conjunction with corollary 3.4.1 (2). □

Corollary 3.9.2. *If P is a prime ideal of A, the prime ideals of the local ring A_P are in one-one correspondence with the prime ideals of A contained in P.*

Proof. Take $S = A - P$ in theorem 3.9 (5). □

Discussion. Thus, the passage from A to A_P eliminates all prime ideals except the ones contained in P. On the other hand, the passage from A to A/P eliminates all prime ideals except the ones containing P (theorem 1.1).
If P, Q are prime ideals with $Q \subseteq P$, then quotienting by Q and localizing at P (in either order, since we know they commute) focuses our attention to those prime ideals which lie between P and Q.
In particular, if $Q = P$, this operation yields a field, called the *residue field at P*. This can also be seen either as the field of fractions of the integral domain A/P, or the residue field of the local ring A_P.

Theorem 3.10. *Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then $S^{-1}(Ann(M)) = Ann(S^{-1}(M))$.*

Proof. First, suppose M is generated by a single element. Then, $M \cong A/Ann(M) \implies S^{-1}M \cong (S^{-1}A)/(S^{-1}Ann(M)) \implies Ann(S^{-1}M) = S^{-1}Ann(M)$.
Next, we show that $Ann(M+N) = Ann(M) \cap Ann(N)$: It is obvious that $Ann(M) \cap Ann(N) \subseteq$

$Ann(M+N)$. On the other hand, $x \in Ann(M+N) \implies x(m+n) = 0 \forall m, n \in M, N \implies x(m+0) = xm = 0 \forall m, xn = 0 \forall n \implies x \in Ann(M) \cap Ann(N) \implies Ann(M+N) \subseteq Ann(M) \cap Ann(N)$, and we are done.
Now, suppose the proposition is true of M, N. Then, $S^{-1}Ann(M+N) = S^{-1}(Ann(M) \cap Ann(N)) = S^{-1}Ann(M) \cap S^{-1}Ann(N) = Ann(S^{-1}M) \cap Ann(S^{-1}N)$ (by hypothesis) $= Ann(S^{-1}M + S^{-1}N) = Ann(S^{-1}(M+N))$. Thus, the proposition will be true of any finitely generated module. □

Corollary 3.10.1. *If N, P are submodules of M and P is finitely generated, then $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$.*

Proof. First, we show that $(N : P) = Ann((N+P)/N) : xP \subseteq N \iff x(N+P) \subseteq N \iff x((N+P)/N) = 0$.
Then, $S^{-1}(N : P) = S^{-1}Ann((N+P)/N) = Ann(S^{-1}(N+P)/N) = \{\frac{a}{s} \in S^{-1}M : (\frac{a}{s})(\frac{p+N}{s}) = 0\} \iff (\frac{a}{s})(\frac{p}{s}) \in S^{-1}N \iff \frac{a}{s} \in (S^{-1}N : S^{-1}P)$, and we are done. □

Theorem 3.11. *Let $f : A \to B$ be a ring homomorphism and P be a prime ideal of A. Then P is the contraction of a prime ideal of $B \iff P^{ec} = P$.*

Proof. First, suppose P is the contraction of a prime ideal; i.e., $P = Q^c$. Then, $P^{ec} = Q^{cec} = Q^c = P$ (by theorem 1.13).
On the other hand, suppose $P^{ec} = P$. Let S be the image of $A - P$ in B. Note that S will be multiplicatively closed. Now, $A - P = A - P^{ec} = A - f^{-1}(P^e) = f^{-1}(B - P^e)$. Then, $x \in f(A-P) = S \implies x \in f \circ (f^{-1}(B - P^e)) \implies x \in B - P^e \implies x \notin P^e \implies P^e \cap S = \emptyset$.
By theorem 3.9, the extension of P^e in $S^{-1}B$ is a proper ideal; it follows that it is contained in a maximal ideal m of $S^{-1}B$. Let $Q = m^c \implies Q \subseteq B$ is prime and $Q \cap S = \emptyset$ (since m is prime). Furthermore, $I \subseteq I^{ec} \implies P^e \subseteq Q \implies P^{ec} = P \subseteq Q^c$.
On the other hand, $x \in Q^c - P \implies f(x) \in Q, f(x) \in f(A-P) = S$, contradicting $Q \cap S = \emptyset$.
Thus, $Q^c \subseteq P$, and we are done. □

Exercises

Presheaves and sheaves:

Let A be a ring and $X = \text{Spec}(A)$, and for $f \in A$, let $X_f = V(f)^C$.

- $\{X_f\}_{f \in A}$ form a basis for $\text{Spec}(A)$:
  For any point $p \in X$, consider an element of the ring which is not in the corresponding prime ideal, $f \notin p$. Then, we will have $p \in X_f$, since $p \notin V(f)$. Thus, the collection covers X.
  Next, let X_f, X_g be basic open sets corresponding to $f, g \in A$, and suppose $p \in X_f \cap X_g \implies p \in V(f)^C, p \in V(g)^C \implies f \notin p, g \notin p \implies fg \notin p$ (since p is prime) $\implies p \notin V(fg) \implies p \in X_{fg}$.
  This proves that the collection forms a basis for the Zariski topology.

For $f \in A$, let $S = \{f^n\}_{n \geq 0}$, and $S^{-1}A = A_f$. Finally, for any basic open set $U = X_f$, define the ring $A(U) = A_f$. We need to check that this is well-defined.

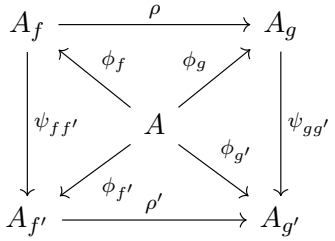
- $A(U)$ depends only on U and not on f:
  Note that $X_f \subseteq X_g \iff V(g) \subseteq V(f) \iff V(r(g)) \subseteq V(r(f)) \iff r((f)) \subseteq r((g))$.
  The first step is clear from the fact that complementation reverses inclusions. The last two steps follow from the fact that the radical of an ideal is the intersection of the prime ideals which contain it.
  Now, suppose $X_f = X_g$. It follows that $r((f)) = r((g))$, so that $g^n = uf, f^m = u'g$ for some $u, u' \in A, n, m \in \mathbb{N}$.
  Then, consider $\phi_f : A \to A_f, \phi_f(a) = \frac{a}{1}$, and let $S = \{g^l\}_{l \geq 0}$, so that $S^{-1}A = A_g$. For any $g^l \in S, \phi_f(g^l)$ is a unit in A_f with inverse $\frac{u'^l}{f^{ml}}$. Next $\phi_f(g^l) = 0 \implies g^l f^k = 0, k \in \mathbb{N}$.
  Thirdly, any element in A_f is of the form $\frac{a}{f^k} = \frac{au^k}{g^{nk}} = \phi_f(au^k)\phi_f^{-1}(g^{nk}), g^{nk} \in S$.
  By corollary 3.2 (universal property of rings of fractions), it follows that $A_f \cong A_g$. We conclude that $A(U)$ is well-defined.

Note that $X = V((1))^C = V(1)^C = X_1$. For $U = X, A(X) = A(X_1) = A_1 = S^{-1}A$, where $S = \{1\}$. In this case, it is clear that the homomorphism $f : A \to A_1, f(x) = \frac{x}{1}$ is also an isomorphism, so that $A(X) \cong A$.

We shall define the *restriction homomorphism* $\rho : A(U) :\to A(U')$ as follows: Let $U' = X_g \subseteq U = X_f$. Then, $r((g)) \subseteq r((f))$, and it follows that $\exists n \in \mathbb{N}$ such that $g^n = uf$. We finally define $\rho(\frac{a}{f^m}) = \frac{au^m}{g^{mn}}$. Sometimes, $\rho(x)$ is denoted by $x|_{U'}$, by analogy with restriction of functions.
It remains to be shown that ρ is well-defined.

- $\frac{a}{f^m} = \frac{b}{f^k} \implies f^q(af^k - bf^m) = 0$, then $g^{nq}(au^m g^{nk} - bu^k g^{mn}) = f^q u^{m+k+q}(af^k - bf^m) = 0 \implies \frac{au^m}{g^{mn}} = \frac{bu^k}{g^{kn}} \implies \rho(\frac{a}{f^m}) = \rho(\frac{b}{f^k})$.

- ρ depends only on U and U':
  Consider the following diagram constituted by various canonical isomorphisms, where $U = X_f = X_{f'}, U' = X_g = X_{g'}$, so that $A(U) = A_f \cong A_{f'}, A(U') = A_g \cong A_{g'}$. Also note that we will have $f'^n = uf, g'^m = vg$ for some $u, v \in A, n, m \in \mathbb{N}$. Also write $g^l = bf, g'^h = cf'$.

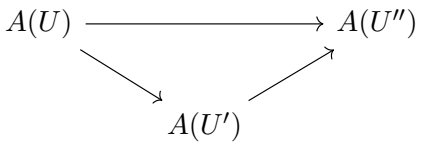


  Here, ϕ_f, ϕ_g, etc. are the natural homomorphism between a ring and its fraction ring. $\psi_{ff'}, \psi_{gg'}$ are the isomorphisms induced by the universal property of fraction rings, so that $\psi_{ff'}(\frac{a}{f^k}) = \phi_{f'}(au^k)\phi_{f'}^{-1}(f'^{nk}) = \frac{au^k}{f'^{nk}}$, and likewise for $\psi_{gg'}$.
  It is easy to check that each of the triangles commute.
  We have defined $\rho'(\frac{a}{f'^m}) = \frac{au'^m}{g'^{mn}}$. If we show that the outer square commutes, our job is done.
  Using the fact that each of the triangles commute, we write $\rho' \circ \phi_{f'} = \phi_{g'} = \psi_{gg'} \circ \phi_g = \psi_{gg'} \circ \rho \circ \phi_f = \psi_{gg'} \circ \rho \circ \psi_{ff'}^{-1} \circ \phi_{f'}$.
  Since $\phi_{f'}$ is surjective, we conclude that $\rho' = \psi_{gg'} \circ \rho\psi_{ff'}^{-1}$; in other words, the square commutes.

The assignment of rings $A(U)$ to each basic open set U of X, along with the restriction homomorphisms ρ, satisfy the following conditions:

1. $U = U' \implies \rho = Id_{A(U)}$.

2. If $U'' \subseteq U' \subseteq U$ are basic open sets, the following diagrams (where the arrows are the restriction homomorphisms) commutes:



Such an assignment of rings, with restriction homomorphisms satisfying the above two conditions, constitutes a *presheaf of rings* on the basis $\{X_f\}_{f\in A}$. The following also holds:

- Let $x \in X$ (so that x is some prime ideal $P \subseteq A$). Then, $A_P \cong \varinjlim_{x\in U} A(U) := A_x$.

  The limit being taken here is the direct limit of a family of rings (for each ring can be regarded as a $\mathbb{Z}$-module).
  To be clear, let $I_x = \{U : U \text{ is a basic open set containing } x\}$, and for $X_f, X_g \in I_x$, define an order $X_f \leq X_g := X_g \subseteq X_f$. For any $X_f \leq X_g, X_{fg} \subseteq X_f, X_g \implies X_{fg} \geq X_f, X_g$. Therefore, I is a directed set.
  Our family of rings is $A(U)_{U\in I} \equiv A(U)_{x\in U}$. Furthermore, the restriction homomorphisms $\rho : A(U) \to A(U')$ satisfy the two requirements for a direct system (by iii and iv).
  Thus, $\mathbf{M}{=}(A(U), \rho_{UU'})$ forms the direct system of $\mathbb{Z}$-modules over which the limit is taken.

This states that the *stalk of the presheaf* at $x \in X, A_x$, is the corresponding local ring A_P. Conceptually speaking, the stalk captures the properties of the sheaf "around" that point. (Notice how, in the direct limit, we move towards rings associated with smaller and smaller neighbourhoods around the point.)

Discussion. Let $(U_i)_{i\in I}$ be a covering of X by basic open sets, and for each $i \in I$ let $s_i \in A(U_i)$ be such that for each $i, j \in I, \rho(s_i) = \rho'(s_j) \in A(U_i \cap U_j)$, where $\rho : A(U_i) \to A(U_i \cap U_j)$ and $\rho' : A(U_j) \to A(U_i \cap U_j)$.

Then, there exists a unique $s \in A(X) = A$ whose image in $A(U_i)$ is $s_i, \forall i \in I$. That is, for each $\rho_i : A \to A(U_i), \rho_i(s) = s_i$.

This fact implies that the presheaf is a *sheaf*.

The existence and uniqueness requirements of s are called *gluing* and *locality*, respectively.

Given two rings, if the restriction (to their intersection) of a pair of elements from each ring agrees, we may call the elements *compatible*. In a sheaf, we can take a collection of pairwise compatible elements and *glue* them all together into a *unique* element s.

Alternatively, locality says that if two elements in $A(X)$ agree on each restriction (given a covering), they must be identical; and gluing says that if there is a collection of elements such that each pair agrees on their domain of overlap ($s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$), then there is an element $s \in A(X)$ whose restriction on U_i is precisely that element.

Primary decomposition

Definition. *An ideal $I \subseteq R$ is primary if $I \neq R$ and $xy \in I \implies x \in I$ or $y^n \in I$ for some $n \in \mathbb{N}$.*
I is primary $\iff R/I \neq 0$ and every zero divisor in R/I is nilpotent.
I is primary if $xy \in I \implies x \in I$ or $y \in I$ or x^n and $y^n \in I$.

Remark. If a prime ideal in a ring is viewed as a generalization of a prime number, a primary ideal is the corresponding generalization of a power of a prime number.

Theorem 4.1. *Let I be a primary ideal in R. Then, $r(I)$ is the smallest prime ideal containing I.*

Proof. We know that the radical of an ideal is the intersection of the prime ideals containing it. Therefore, it suffices to show that $r(I)$ is prime.
Let $xy \in r(I) \implies (xy)^m \in I \implies x^m \in I$ or $y^{mn} \in I \implies x \in r(I)$ or $y \in r(I) \implies r(I)$ is prime. □

Remark. If the radical of a primary ideal Q is the prime ideal P, then Q is said to be *P-primary.*

Example. Consider the three following examples.

- In $\mathbb{Z}$, the primary ideals are precisely (0) and (p^n), where p is prime.
  $ab \in (p^n) \implies p^n \mid ab$. $p^n \nmid a \implies p \mid b \implies p^n \mid b^n \implies b^n \in (p^n)$ (this can be easily proven using the fundamental theorem of arithmetic), so that (p^n) is primary.
  On the other hand, if $r(I) \neq 0$ is prime, then I must be primary. For suppose $I = (p^n q^m) \implies I \subseteq (p), (q)$. Then, $r(I) \subseteq (p) \cap (q) \implies pq \in r(I)$ but $p \notin r(I), q \notin r(I)$, a contradiction.

- However, not all primary ideals are prime powers.
  Let $R = k[x, y]$ and $Q = (x, y^2)$. Then $R/Q \cong k[y]/(y^2) \neq 0$. Furthermore, zero divisors in R/Q will all be multiples of y; therefore, they will be nilpotent. Thus, Q is primary.
  Now, $r(Q) = P = (x, y)$, so that $P^2 \subset Q \subset P$, where the inclusions are strict. We thus see that Q is not a prime power. (If $Q = P'^n$ for some other prime ideal, then $r(Q) = P' \implies P' = P$, which is then a contradiction.)

- Conversely, not all prime powers are primary ideals.
  Let $R = k[x, y, z]/(xy - z^2)$ and $P = (\bar{x}, \bar{z})$, where $\bar{x}$ is the image of x in R. Now, $R/P \cong k[x, y, z]/(x, z, xy - z^2) \cong k[y]$, which is an integral domain; thus, P is prime.
  However, P^2 is not primary: $\bar{x}\bar{y} = \bar{z}^2 \in P^2$, but $\bar{x} \notin P^2, \bar{y} \notin r(P^2) = P$.

Theorem 4.2. *If $r(I)$ is maximal, I is primary.*

Proof. Let $r(I) = M$. The image of M in R/I is the nilradical of R/I. It is also a maximal ideal of R/I. Since the nilradical is the intersection of all prime ideals of R/I, we conclude that R/I has only one prime ideal, which is the image of M.
Now, if an element is in this image, it is nilpotent; if not, it is a unit (recall corollary 1.4.2). If an element is a zero divisor, it cannot be a unit. Therefore, all zero divisors in R/I are nilpotent, and we conclude that I is primary. □

Corollary 4.2.1. *The powers of a maximal ideal M are M-primary.*

Proof. Follows from the fact that $r(P^n) = P$ for a prime ideal. □

Lemma 4.3. *If $\{Q_i\}_{i=1}^n$ are P-primary, then $Q = \bigcap_{i=1}^n Q_i$ is P-primary.*

Proof. $r(Q) = r(\bigcap_{i=1}^n Q_i) = \bigcap_{i=1}^n r(Q_i) = P$. (It is easy to check that $r(A \cap B) = r(A) \cap r(B)$.) Next, let $xy \in Q, y \notin Q$. Then, for some $i, xy \in Q_i, y \notin Q_i \implies x^n \in Q_i \implies x \in P \implies x^n \in Q$. □

Lemma 4.4. *Let Q be a P-primary ideal in R and $x \in R$. Then:*

1. $x \in Q \implies (Q : x) = R$
2. $x \notin Q \implies (Q : x)$ *is P-primary*
3. $x \notin P \implies (Q : x) = Q$.

Proof. $(Q : x) = \{a \in R : ax \in Q\}$.

1. Since $x \in Q$, this will be true for all $a \in R$.
2. $y \in (Q : x) \implies xy \in Q \implies y^n \in Q \implies y \in P$, since $x \notin Q$. Thus, $Q \subseteq (Q : x) \subseteq P \implies r(Q : x) = P$.
   Also suppose, $yz \in (Q : x), y \notin P$. Then $xyz \in Q \implies xz \in Q \implies z \in (Q : x)$.
3. $x^n \notin Q, ax \in Q \implies a \in Q$. Thus, $(Q : x) = Q$.

□

Discussion. A *primary decomposition* of an ideal $I \subseteq R$ is an expression of I as a finite intersection of primary ideals:

$$I = \bigcap_{i=1}^{n} Q_i$$

In general, such a primary decomposition need not exist for an ideal. If it does, we call the ideal *decomposable*. There are special kinds of rings called *Noetherian rings* in which every ideal is decomposable.

If, furthermore,

- The $r(Q_i)$ are all distinct
- $\bigcap_{j \neq i} Q_j \not\subseteq Q_i$

then, the primary decomposition is said to be *minimal/irredundant/reduced/normal.*

Given a primary decomposition, we can use lemma 4.3 to combine ideals as required and achieve the first condition. If we then drop the superfluous terms to satisfy the second condition, we can turn any given primary decomposition into a minimal one.

Theorem 4.5 (First Uniqueness Theorem)**.** *Let I be a decomposable ideal and $I = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition; and let $P_i = r(Q_i)$.*
Let $S = \{r(I : x) \mid x \in R\}$. Then, $\{P_i\}$ are precisely the prime ideals which occur in S. Thus, they are independent of the particular decomposition of I.

Proof. It is easy to check that $\bigcap(I_i : x) = (\bigcap I_i : x)$. Then, $(I : x) = (\bigcap Q_i : x) = \bigcap(Q_i : x) \implies r(I : x) = \bigcap_{i=1}^{n} r(Q_i : x) = \bigcap_{x \notin Q_j} P_j$, by lemma 4.4 (1), (2). Now, suppose $r(I : x)$ is prime. Then, by theorem 1.11, $r(I : x) = P_j$ for some j.
Conversely, for each i we have some $x_i \notin Q_i, x_i \in \bigcap_{j \neq i} Q_j$, since the decomposition is minimal. Then, by the previous equation, we have $r(I : x_i) = P_i$. □

Remark. This is equivalent to saying that $\{P_i\}$ are precisely the prime ideals which are radicals of annihilators of elements in the module R/I.

Example. Let $R = k[x, y], I = (x^2, xy)$. Let $P_1 = (x), P_2 = (x, y), P_3 = (x^2, y)$ Note that P_2 will be a maximal ideal (Nullstellensatz). Therefore, P_2^2 is a primary ideal. Since k is a field and x is an irreducible polynomial, P_1 is a prime (and thus primary) ideal. I itself is not primary, since $\bar{y}$ is a zero-divisor in R/I but not nilpotent. Finally, P_3 is primary since if $\bar{a}\bar{p} = 0, \bar{p} \neq 0$ in R/P_3 then $a(x, y)p(x, y) \in P_3 \implies \bar{a} = 0$ by a having a factor of y, or a has a factor of x, making $\bar{a}$ nilpotent.

$$I = P_1 \cap P_2^2 = P_1 \cap P_3 \text{ and } r(I) = P_1 \cap P_2 = P_1.$$

Note, first of all, that the primary components are not independent of the decomposition; we have given two distinct minimal primary decompositions above.

The prime ideals $\{P_i\}$ given by the radicals of the primary ideals in the decomposition are said to *belong* to I, or be *associated* with I, and I will be primary iff it has exactly one associated prime ideal. The minimal elements of $\{P_1, ..., P_n\}$ are called the *minimal* or *isolated* prime ideals belonging to I, and the others are called *embedded* prime ideals. In the above example, P_1 is minimal and P_2 is embedded.

There is some geometric context behind the names 'isolated' and 'embedded'. Let $R = k[x_1, ...x_n]$, where k is a field, and $I \subseteq R$ be an ideal. I will give rise to a variety $X \subseteq k^n$ (the set of points at which all the polynomials in I vanish).

The minimal primes belonging to I correspond to the *irreducible components* of X; that is, a subvariety of X which cannot be written as the union of two varieties.

The embedded primes belonging to I correspond to subvarieties of the above; that is, to varieties embedded in the irreducible components. In the above example, the embedded ideal (x, y) corresponds to the origin $(0, 0)$. The irreducible component as well as the variety are both defined by the line $x = 0$.

Theorem 4.6. *Let I be a decomposable ideal. Then any prime ideal $I \subseteq P$ contains a minimal prime ideal belonging to I.*

Proof. Let $\bigcap_{i=1}^{n} Q_i = I \subseteq P$. Then, $r(\bigcap Q_i) = \bigcap r(Q_i) = \bigcap P_i \subseteq r(P) = P$. By theorem 1.11, $P_i \subseteq P$ for some i, so that P contains some minimal prime ideal of I. □

Corollary 4.6.1. *The minimal prime ideals of I are the minimal elements in the set of all prime ideals containing I.*

Proof. $I = \bigcap_{i=1}^{n} Q_i \subseteq \bigcap_{i=1}^{n} P_i \implies I \subseteq P_i$ for all i, which means I is contained in each of its minimal prime ideals. The conclusion follows from this and theorem 4.6. □

Remark. It is easy to see that the set of nilpotent elements N of a ring, being the intersection of all its prime ideals, will be the intersection of all the minimal primes belonging to 0 (which is another way of saying the intersection of the smallest prime ideals of a ring).

Theorem 4.7. *Let I be a decomposable ideal with $I = \bigcap_{i=1}^{n} Q_i, P_i = r(Q_i)$. Then*

$$\bigcup_{i=1}^{n} P_i = \{x \in R : (I : x) \neq I\}$$

In particular, if the zero ideal is decomposable, then the set of zero-divisors of R, D, equals the union of the prime ideals belonging to 0.

Proof. The primary decomposition of $\bar{0} \in R/I$ will be $\bar{0} = \bigcap_{i=1}^{n} \bar{Q}_i$. We first show that the set of zero divisors of R/I equals the union of the prime ideals belonging to $\bar{0}$.
We know $D = \bigcup_{x \neq \bar{0}} r(\bar{0} : x)$ from theorem 1.12 (2) (here, $x \in R/I$). Also, we have seen that $r(\bar{0} : x) = \bigcap_{x \notin \bar{Q}_j} \bar{P}_j \subseteq \bar{P}_j$ for some j. Therefore, $D \subseteq \bigcup_{i=1}^{n} \bar{P}_i$. But since we also know from theorem 4.5 that each $\bar{P}_i$ is of the form $r(\bar{0} : x)$ for some $x \in R/I$, we have $\bigcup_{i=1}^{n} \bar{P}_i \subseteq D$.

So, we have shown that $\bigcup_{i=1}^{n} \bar{P}_i = \{x \in R/I : (\bar{0} : x) \neq \bar{0}\}$. It follows that $\bigcup_{i=1}^{n} P_i = \bigcup_{i=1}^{n} (P_i + I) = \bigcup_{i=1}^{n} \pi^{-1}(\bar{P}_i) = \pi^{-1}(\bigcup_{i=1}^{n} \bar{P}_i) = \pi^{-1}(\{x \in R/I : (\bar{0} : x) \neq \bar{0}\}) = \{x \in R : (I : x) \neq I\}$, and we are done. □

Theorem 4.8. *Let S be a multiplicatively closed subset of A and Q be a P-primary ideal.*

1. *$S \cap P \neq \emptyset \implies S^{-1}Q = S^{-1}A$*
2. *$S \cap P = \emptyset \implies S^{-1}Q$ is $S^{-1}P$-primary and its contraction in A is Q.*

Proof. We prove each part in turn.

1. Suppose $s \in S \cap P$. Then, $s^n \in S \cap Q$ for some $n \in \mathbb{N}$. Thus, $\frac{s^n}{1} \in S^{-1}Q$. Since this is a unit in $S^{-1}A$, the conclusion follows.

2. Suppose $S \cap P = \emptyset$. Then, $s \in S, as \in Q \implies a \in Q$, since $s \in S \implies s \notin P \implies s^n \notin Q$. In other words, $\bigcup_{s \in S} (Q : s) = Q$. Now, by theorem 3.9 (2), $\bigcup_{s \in S} (Q : s) = Q^{ec} \implies Q = Q^{ec}$.
   It remains to be shown that $S^{-1}Q = Q^e$ is $S^{-1}P$-primary. But also by theorem 3.9 (6), $r(Q^e) = r(S^{-1}Q) = S^{-1}r(Q) = S^{-1}P$. Finally, suppose $\frac{xy}{st} \in S^{-1}Q \implies \frac{xy}{st} = \frac{z}{u}, z \in Q, u \in S$. It suffices to show that either $x \in Q$ or $y^n \in Q$. Now, the above tells us that $xyuv \in Q$ for some $v \in S$. Therefore, either $xuv \in Q$ or $y^n \in Q$. But $xuv \in Q \implies x \in Q$ (by the above), since $uv \in S$. Hence, proved.

□

Remark. Note that the contraction of a primary ideal will be a primary ideal. It follows that the primary ideals of $S^{-1}A$ are in one-one correspondence with the primary ideals of A whose radical doesn't meet S.

Henceforth, we shall denote the contraction of $S^{-1}I = I^e$ in R as simply $S(I)$.

Theorem 4.9. *Let S be a multiplicatively closed subset of A, I be a decomposable ideal with $I = \bigcap_{i=1}^{n} Q_i$ being a minimal primary decomposition, and $P_i = r(Q_i)$. Number the Q_i so that S meets each of $\{P_{m+1}, ..., P_n\}$ but none of $\{P_1, ..., P_m\}$. Then,*

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i, \quad S(I) = \bigcap_{i=1}^{m} Q_i$$

are minimal primary decompositions.

Proof. $S^{-1}I = \bigcap_{i=1}^{n} S^{-1}Q_i$ (by 3.9) $= \bigcap_{i=1}^{m} S^{-1}Q_i$, wherein $S^{-1}Q_i$ is $S^{-1}P_i$-primary for $i = 1, ..., m$. (by 4.8 (1) & (2) respectively). Since the P_i are distinct, so are the $S^{-1}P_i$. The second condition for minimality follows from the fact that $I \subsetneq J \implies S^{-1}I \subsetneq S^{-1}J$. Thus, the primary decomposition is also minimal.
Contracting both sides, $S(I) = (S^{-1}I)^c = \bigcap_{i=1}^{m}(S^{-1}Q_i)^c = \bigcap_{i=1}^{m} Q_i$ (by 4.8 (2)). □

Definition. *A set Σ of prime ideals belonging to I are said to be isolated if it satisfies the following condition:*
If P' is a prime ideal belonging to I and $P' \subseteq P$ for some $P \in \Sigma$, then $P' \in \Sigma$.

Remark. There is a slight ambiguity in the text. We say that P is a minimal prime, but that $\{P\}$ is an isolated set of primes (for a minimal prime P): To be isolated is a property of a set of primes, not of a prime ideal itself.

Theorem 4.10 (Second Uniqueness Theorem)**.** *Let $I = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of I, and let $\{P_{i_1}, ..., P_{i_m}\}$ be an isolated set of prime ideals belonging to I. Then $Q_{i_1} \cap ... \cap Q_{i_m}$ is independent of the decomposition.*

Proof. Let $S = R - (P_{i_1} \cup P_{i_2} ... \cup P_{i_m})$. Clearly, S does not meet $P_{i_1}, ..., P_{i_m}$. Furthermore, S will meet each of the prime ideals belonging to I which are not in this set: For suppose $P \notin \{P_{i_1}, ..., P_{i_m}\}$ and $P \cap S = \emptyset \implies P \subseteq P_{i_1} \cup ... \cup P_{i_m} \implies P \subseteq P_{i_k}$ for some k (by theorem 1.11), which contradicts the definition of an isolated set.
Thus, from 4.9, $Q_{i_1} \cap ... \cap Q_{i_m} = S(I)$, from which independence follows. □

Corollary 4.10.1. *The primary components corresponding to minimal prime ideals in a decomposition are uniquely determined by I.*

Remark. The embedded primary components are not, in general, uniquely determined by I. In fact, if R is a Noetherian ring, there are infinitely many choices for each embedded component.