3. Prime and maximal ideals

3.1. Definitions and Examples.

Definition. An ideal P in a ring A is called *prime* if $P \neq A$ and if for every pair x, y of elements in $A \backslash P$ we have $xy \notin P$. Equivalently, if for every pair of ideals I, J such that $I, J \not\subset P$ we have $IJ \not\subset P$.

Definition. An ideal $\mathfrak{m}$ in a ring A is called *maximal* if $\mathfrak{m} \neq A$ and the only ideal strictly containing $\mathfrak{m}$ is A.

Exercise.

(1) An ideal P in A is prime if and only if A/P is an integral domain.
(2) An ideal $\mathfrak{m}$ in A is maximal if and only if $A/\mathfrak{m}$ is a field.

Of course it follows from this that every maximal ideal is prime but not every prime ideal is maximal.

Examples.

(1) The prime ideals of $\mathbb{Z}$ are (0),(2),(3),(5),...; these are all maximal except (0).
(2) If $A = \mathbb{C}[x]$, the polynomial ring in one variable over $\mathbb{C}$ then the prime ideals are (0) and $(x - \lambda)$ for each $\lambda \in \mathbb{C}$; again these are all maximal except (0).
(3) If $A = \mathbb{Z}[x]$, the polynomial ring in one variable over $\mathbb{Z}$ and p is a prime number, then (0), (p), (x), and $(p, x) = \{ap + bX | a, b \in A\}$ are all prime ideals of A. Of these, only (p, x) is maximal.
(4) If A is a ring of R-valued functions on a set for any integral domain R then $I = \{f \in A | f(x) = 0\}$ is prime.

Exercise. What are the prime ideals of $\mathbb{R}[X]$? What can you say about the prime ideals of $k[X]$ for a general field k?

As we will see as the course goes on — and you might already guess from these examples — prime ideals are central to all of commutative algebra.

In modern algebraic geometry the set of prime ideals of a ring A is viewed as the points of a space and A as functions on this space. The following lemma tells us that in this viewpoint a ring homomorphism $f \colon A \to B$ defines a function from the space associated to B to the space associated to A. At first sight this reversal of direction may seem perverse but it is one of those things we have to live with.

Suppose that $f \colon X \to Y$ is a function then we may define a ring homomorphism $f^* \colon R^Y \to R^X$ by $f^*(\theta) = \theta \circ f$. Notice also, for example that if f is continous then f restricts to a ring homomorphism $C(Y) \to C(X)$.

The following lemma is attempt at a converse to this.

Lemma. *If $f \colon A \to B$ is a ring homomorphism and P is a prime ideal of B, then $f^{-1}(P)$ is a prime ideal of A.*

Proof. Notice that f induces a ring homomorphism g from A to B/P by post-composing with the natural projection map $B \to B/P$. Now $a \in \ker g$ if and only if $f(a) \in P$, so using the first isomorphism theorem we see that g induces an isomorphism from $A/f^{-1}(P)$ to a subring of B/P. Since the latter is an integral domain, $A/f^{-1}(P)$ must be an integral domain too. □

Note that the above lemma isn't true if we replace the word prime by maximal everywhere. For example if we consider the inclusion $\iota : \mathbb{Z} \to \mathbb{Q}$ then (0) is a maximal ideal in $\mathbb{Q}$ but $\iota^{-1}(0) = (0)$ is not maximal in $\mathbb{Z}$.

If we want to put prime ideals at the centre of commutative algebra then an obvious question to ask is 'must a ring have any prime ideals?'

In order to demonstrate that the answer to this question is positive, we need to recall Zorn's lemma.

Zorn's Lemma. *If $(S, \leq)$ is a partially ordered set such that every chain C in S has an upper bound in S then for every element x in S there is a maximal element y in S with $x \leq y$.*

This result follows from the Axiom of Choice. Indeed, as those who know what the Axiom of Choice is will probably already know, in the usual axiomatisation of set theory the two are equivalent. As a result, we will assume the Axiom of Choice holds.

Now we can prove,

Theorem. *If A is a ring and I an ideal of A such that $I \neq A$, then A contains a maximal ideal $\mathfrak{m}$ such that $I \subset \mathfrak{m}$.*

Note that if A isn't the zero ring then $I = (0)$ is an ideal not equal to A so it follows from this that there is always at least one maximal ideal.

Proof. Let $\mathcal{A}$ be the set of ideals of A not equal to A, ordered by inclusion. We must show that whenever $\mathcal{C}$ is a chain in $\mathcal{A}$ it has an upper bound in $\mathcal{A}$, since then the result follows immediately from Zorn. So let's take such a chain $\mathcal{C}$.

Let $I = \bigcup_{J \in \mathcal{C}} J$. Now suppose x_1, x_2 are in I. Then there are J_1, J_2 in $\mathcal{C}$ such that $x_i \in J_i$. Either $J_1 \subset J_2$ or $J_2 \subset J_1$; WLOG the former. Then $x_1 \in J_2$, so $x_1 + x_2 \in J_2 \subset I$. Also if $a \in A$ then $ax_i \in J_2 \subset I$ for each i. It follows that I is an ideal.

It now just remains to check that $I \neq A$. But $1 \notin J$ for each $J \in \mathcal{C}$, so $1 \notin I$ and $I \neq A$ as required. □

Once we have defined Noetherian rings, it will be apparent that we do not need Zorn's lemma to prove this result for that important class of rings.

Corollary. *Every non-unit lies in a maximal ideal.*

Proof. If x is a non-unit then $(x) \neq A$ □

Consider the ring $\mathbb{C}(x)$ of rational functions $\{\frac{f(x)}{g(x)} | g \neq 0\}$ on $\mathbb{C}$. And let A be the subring of $\mathbb{C}(x)$ consisting of those functions with no pole at 0 ie $\{\frac{f}{g} | g(0) \neq 0\}$. We may consider A as 'polynomial functions on $\mathbb{C}$ defined "near" 0'.

Now f is a unit in A precisely if $f(0) \neq 0$, and the set of non-units of A form an ideal: the kernel of evaluation at 0. We will see in a moment that this is the unique maximal ideal of A.

Definition. A ring A with precisely one maximal ideal $\mathfrak{m}$ is called a *local ring.* In this case that field $A/\mathfrak{m}$ is called *the residue field* of A.

Proposition. *A ring A is local if and only if the set of non-units in A form an ideal in A.*

Proof. Suppose that A is local. Then since every non-unit lies in a maximal ideal and there is only one maximal ideal $\mathfrak{m}$, they must all lie in $\mathfrak{m}$. Moreover $\mathfrak{m}$ cannot contain any units since then $\mathfrak{m}$ would have to be the whole of A. So $\mathfrak{m}$ is the set of non-units in A.

Conversely, suppose that the set of non-units in A form an ideal I, and J is any ideal not equal to A. Then J again cannot contain any units so $J \subset I$ and I is the unique maximal ideal. □

Corollary. *Let A be a ring with maximal ideal $\mathfrak{m}$. If every element of $1+\mathfrak{m}$ is a unit, then A is a local ring.*

Proof. Let $x \in A\backslash\, \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the smallest ideal containing $\mathfrak{m}$ and x is A. It follows that $1 = ax + y$ for some $a \in A$ and $y \in \mathfrak{m}$. Then $ax = 1 - y$ is a unit by assumption and so $\mathfrak{m}$ contains all the non-units. □

3.2. **The prime spectrum.**

Definition. Given a ring A we define $\mathrm{Spec}(A)$ to be the set of all prime ideals of A. We also define $\mathrm{maxSpec}(A)$ to be the set of all maximal ideals of A.

We want to put a topology on these spaces. To this end, for each subset S of A we define $V(S)$ to be the set of prime ideals of A containing S. These will be the closed sets of $\mathrm{Spec}(A)$. We will then give $\mathrm{maxSpec}(A)$ the subspace topology. We'll call these the *Zariski topology.*

The following lemma will convince us that this does indeed define a topology:

Lemma. *(i) If I is the smallest ideal containing S then $V(S) = V(I)$;*
(ii) $V(\{0\}) = \mathrm{Spec}(A)$,$V(\{1\}) = \emptyset$;
(iii) if $(E_\gamma)_{\gamma\in\Gamma}$ is a family of subsets of A, then

$$V\left(\bigcup_{\gamma\in\Gamma} E_\gamma\right) = \bigcap_{\gamma\in\Gamma} V(E_\gamma);$$

(iv) if I and J are ideals in A then $V(I\cap J) = V(I)\cup V(J)$.

Note that (ii) tells us that $\mathrm{Spec}(A)$ and the empty set are closed, (iii) that the closed sets are closed under arbitrary intersections and (iv) together with (i) that they are closed under finite unions. We call the topology on $\mathrm{Spec}(A)$ with these closed sets the *Zariski topology.*

Proof. (i) Since $S \subset I$ it is clear that $V(I) \subset V(S)$. If any ideal contains S then it also contains I and so $V(S) \subset V(I)$.

(ii) and (iii) are clear from the definition.

(iv) Every ideal containing either I or J must contain $I \cap J$, and so we have $V(I) \cup V(J) \subset V(I \cap J)$. Suppose that $P \in \mathit{Spec}(A)$ and $I \cap J \subset P$ then $IJ \subset P$ so by primality of P either $I \subset P$ or $J \subset P$. □

Exercise. Draw pictures of $\mathrm{Spec}(\mathbb{C}[x])$, $\mathrm{Spec}(\mathbb{R}[x])$ and $\mathrm{Spec}(\mathbb{Z})$.

Recall that $N(A)$ is the ideal consisting of all nilpotent elements of A.

Proposition. *The nilradical of A is the intersection of all the prime ideals of A.*

Note this means that $V(S) = \mathrm{Spec}(A)$ if and only if $S \subset N(A)$. In particular there is a natural bijection $\mathrm{Spec}(A) \leftrightarrow \mathrm{Spec}(A/N(A))$.

Proof. Suppose that $f \in N(A)$, so $f^n = 0$ for some positive integer n. Now if P is any ideal then $f^n \in P$ so if P is prime then f^{n-1} is in P or f is in P. Inductively we see that in either case f is in P. It follows that f is in every prime ideal and $N(A)$ is contained in the intersection of all prime ideals.

Conversely, suppose f isn't nilpotent, and consider the set $\mathcal{A}$ of ideals I in A such that f^n is not in I for every positive integer n. Since f isn't nilpotent, (0) is in $\mathcal{A}$ and so by Zorn $\mathcal{A}$ has a maximal element I_0.

We claim that I_0 is prime. Suppose a, b are in $A \backslash I_0$. Then there is an n such that f^n is in the ideal $I_0 + (a)$ and an m such that f^m is in $I_0 + (b)$. It follows that $f^{n+m} \in I_0 + (ab)$. By definiton of I_0 this must be strictly bigger than I_0 and so ab is not an element of I_0 and the claim holds.

Since f is not in I_0, it now follows that f is not in the intersection of all prime ideals and so $N(A)$ contains the intersection of all prime ideals as required. □

Definition. Given any ideal I of A, we define the *radical of* I,

$$\sqrt{I} = \{x \in A | x^n \in I \text{ for some } n > 0\} = \pi^{-1}(N(A/I))$$

Corollary. *The radical of an ideal of I is the intersection of all the prime ideals containing I.*

Proof. We just apply the previous proposition to the ring A/I. □

We see from this that for any ideal I we have $V(I) = V(\sqrt{I})$.

Also of interest later will be the Jacobson radical of a ring:

Definition. Let A be a non-zero ring then the *Jacobson radical* of A, $\mathrm{Jac}(A)$, is the intersection of all maximal ideals of A.

Note that always $N(A) \subset \mathrm{Jac}(A)$. We will see later that algebraically Hilbert's famous Nullstellensatz says that for finitely generated algebras A over $\mathbb{C}$ we have $N(A) = \mathrm{Jac}(A)$.

We can characterise the Jacobson radical as follows:

Lemma. $\mathrm{Jac}(A) = \{a \in A | 1 - ax \text{ is a unit in } A \text{ for all } x \in A\}$.

Proof. If $a \in \mathrm{Jac}(A)$ and $1 - ax$ is not a unit in A for some $x \in A$ then $1 - ax$ is contained in some maximal ideal $\mathfrak{m}$ of A (by the Zorn argument earlier). But a must also be an element of $\mathfrak{m}$ so $1 - ax + ax = 1 \in \mathfrak{a}$, a contradiction.

Conversely if $a \notin \mathrm{Jac}(A)$ then there is a maximal ideal $\mathfrak{m}$ not containing a. Thus $\mathfrak{m} + (a) = A$ and $1 = y + ax$ for some $y \in \mathfrak{m}$ and $x \in A$. Thus $1 - ax \in \mathfrak{m}$ cannot be a unit. □

Lemma. *Let $\phi\colon A \to B$ be a ring homomorphism, and write $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$. Recall that if $P \in Y$ then $\phi^{-1}(P) \in X$, and write ϕ^* for the mapping from Y to X induced in this way. Then*

(i) *ϕ^* is continuous.*
(ii) *If ϕ is a surjection then ϕ^* is a homeomorphism onto $V(\ker \phi)$. In particular $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A/N(A))$ are naturally homeomorphic.*
(iii) *If $\psi : B \to C$ is also a ring homomorphism then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.*

Proof. (i) it suffices to show that if I is an ideal in A then $\phi^{*-1}(V(I))$ is closed in Y. Now $V(I)$ is the set of prime ideals in A containing I, so a prime ideal P in B is in $\phi^{*-1}(V(I))$ if and only if $\phi^*(P)$ contains I if and only if $\phi^{-1}(P)$ contains I if and only if P contains $\phi(I)$. So $\phi^{*-1}(V(I)) = V(\phi(I))$ which is closed as required.

(ii) Suppose ϕ is a surjection. We may assume that $B = A/\ker\phi$. Then the isomorphism theorems for rings give us a 1-1 order preserving correspondence between ideals of B and an ideals of A containing $\ker\phi$. Moreover this induces a correspondence between prime ideals of B and prime ideals of A containing $\ker\phi$ this latter correspondence may be described by ϕ^*. Thus ϕ^* is a bijection from $\mathrm{Spec}(B)$ to $V(\ker\phi)$. The order preserving property makes it easy to see that it is in fact a homeomorphism.

(iii) This just follows from the fact that $(\psi\circ\phi)^{-1}(Q) = \phi^{-1}(\psi^{-1}(Q))$ for each prime ideal Q in C. □

Note for category theorists in the audience: the final part of this lemma tells us that we have a contravariant functor from rings and ring homomorphisms to topological spaces and continuous maps given by A maps to $\mathrm{Spec}(A)$ and ϕ maps to ϕ^*. This defines an equivalence of categories between (commutative) rings and affine schemes [or rather its opposite].

4. Universal Properties

4.1. **Free modules.**

Qn. What does it mean to say that a k-vector space V has a basis X?

Answer (1). $X \subset V$ is linearly independent and spans V.

Answer (2). Alternatively, for every k-vector space W and every function $f\colon X \to W$ extends uniquely to a linear map $\alpha\colon V \to W$. (LI is loosely equivalent to extends and spans is equivalent to extends in at most one way).

We might say that there is a canonical bijection $\{f\colon X \to W\} \to \mathrm{Hom}_k(V, W)$ for all k-vector spaces W.

We know that two vector spaces with bases of the same cardinality are isomorphic.

Why? If we have (X, V) as above and (X', V') another such pair and $\pi\colon X \to X'$ is a bijection then by the above we have unique linear maps $\alpha\colon V \to V'$ and $\beta\colon V' \to V$ extending ϕ and ϕ^{-1} (there is an abuse of notation here but that should not concern us too much).

But now $\beta\alpha\colon V \to V$ is extending $\phi^{-1}\phi = \mathrm{id}_X$ and so must be id_V since this extends id_X. Similarly $\alpha\beta\colon V' \to V'$ extends $\phi\phi^{-1} = \mathrm{id}_{X'}$ and so must be $\mathrm{id}_{V'}$. So α and β are mutual inverses.

Diagramatically,

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[d, "\phi"] \arrow[dd, bend right=60, "\mathrm{id}"'] & V \arrow[d, dashed, "\exists!\alpha"] \arrow[dd, bend left=60, "id"] \\
X' \arrow[r, hook] \arrow[d, "\phi^{-1}"] & V' \arrow[d, dashed, "\exists!\beta"] \\
X \arrow[r, hook] & V
\end{tikzcd}$$

Since the big rectangle commutes the identity must be the unique map that makes it commute but the two smaller squares commute so $\beta\alpha = \mathrm{id}$.

Now it is natural to change the defintion of a vector space with a basis slightly.

Answer (3). If V is a k-vector space, we say an injection $\iota\colon X \to V$ is a basis for V if for every k-vector space W and every function $f\colon X \to W$, $\exists!$ linear map $g\colon V \to W$ making

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr, "f"'] & V \arrow[d, dashed, "g"] \\
& W
\end{tikzcd}$$

commute.

Identifying X and X' above under ϕ we have seen that if $\iota\colon X \to V$ and $\iota'\colon X' \to V'$ are bases for V and V' then there is a canonical isomorphism $V \to V'$ depending only on ι and ι'.

Notice however:

(i) in our discussion we have not shown that for every set X there is a vector space with basis X;
(ii) we certainly haven't shown that every vector space has a basis.

But if we can prove (i) then we will be able to speak of 'the vector space with basis X.'

More generally,

Definition. Suppose that A is a ring and X a set, we say an A-module $A^{(X)}$ (together with an injection $\iota\colon X \to A^{(X)}$) is the *free A-module on X* if for every A-module M and every function $f\colon X \to M$ there exists a unique A-module map $\alpha\colon A^{(X)} \to M$ making

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr, "f"'] & A^{(X)} \arrow[d, dashed, "\exists!\alpha"] \\
& M
\end{tikzcd}$$

commute.

We have seen that this definition characterises the pair $(A^{(X)}, \iota)$ up to unique isomorphism if it exists. In fact $\{\theta \in A^X | \theta(x) = 0 \text{ for all but finitely many } x \in X\}$ together with the function ι that sends $x \in X$ to the characteristic function of x satisfies the universal property for a free module. So for every set X there is a free A-module on X. Of course not every A-module is free in general.

4.2. **Localisation.** Algebraically, localisation involves inverting elements of a ring.

Geometrically, this corresponds to concentrating on open subsets of our space.

Example. $\mathbb{C}[x]$ corresponds to polynomial functions on $\mathbb{C}$.

(1) If we invert x we obtain $\mathbb{C}[x, x^{-1}]$ which corresponds to polynomial functions on $\mathbb{C}\backslash\{0\}$.
(2) If we invert all elements of $\mathbb{C}[x]$ not contained in (x) we get rational functions on $\mathbb{C}$ with no pole at 0 i.e. polynomial functions defined on a neighbourhood of 0 in $\mathbb{C}$.
(3) We may interpret $\mathbb{C}(x)$ as polynomial functions on the generic point (0) of $\operatorname{Spec}(\mathbb{C}[x])$.

The classical example of localisation is the construction of the rationals from the integers. In this case we invert all non-zero elements of $\mathbb{Z}$. The goal of this section is to generalise this construction to inverting arbitrary subsets. But if we invert x and y then we have *de facto* inverted xy too. Thus

Definition. Suppose that A is a ring. A subset S of A is called multiplicatively closed (m.c. for short) if $1 \in S$ and S is closed under multiplication.

We aim to construct a new ring A_S from A so that all elements of S become units in a maximally efficient way. In particular we want A_S to satisfy:
There is a ring homomorphism $\iota\colon A \to A_S$ such that

- $\iota(s)$ is a unit in A_S for all $s \in S$;
- if $g\colon A \to B$ is a ring homomorphism such that $g(s)$ is a unit in B for each $s \in S$ then there exists a unique ring homomorphism $h : A_S \to B$ such that the following diagram commutes

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[d, "g"] & A_S \arrow[dl, dashed, "h"] \\
B. &
\end{tikzcd}$$

By the argument used for free modules if such a pair (A_S, ι) exists then it does so uniquely up to unique isomorphism.

We now explain how to construct such a ring: first we define an equivalence relation on the set $A \times S$ by $(a, s) \sim (b, t)$ precisely if there is a $u \in S$ such that $(at - bs)u = 0$ for some $u \in S$.

Lemma. *This is an equivalence relation.*

Proof. Reflexivity and symmetry are evident. We need to check transitivity: suppose $(a, s) \sim (b, t) \sim (c, u)$ so there are v, w in S such that $(at - bs)v = (bu - ct)w = 0$. Then

$$atvuw = bsvuw = ctsvw$$

so $(au - cs)tvw = 0$ and $tvw \in S$ as required. □

We write, with deliberate suggestiveness, a/s for the equivalence class containing (a, s) and A_S for the set of equivalence classes.

Notice that if S contains zero-divisors in A then we cannot prove transitivity of the more straightforward relation $(a, s) \approx (b, t)$ precisely if $at = bs$. If A is an integral domain then the two relations are the same.

We still need to put a ring structure on A_S. We do this using the usual 'fractional calculus'; that is we define $a/s + b/t = (at + bs)/st$ and $(a/s)(b/t) = (ab)/(st)$.

Dull Exercise. Show that these operations are independent of the choice of equivalence class representatives (a, s) and (b, t) and that they satisfy the axioms of a ring. Show, moreover, that the function $\iota : A \to A_S$ that maps a to $a/1$ is ring homomorphism. Finally $\ker \iota = \{a \in A | as = 0 \text{ for some } s \in S\}$.

Notice ι need not be an injection: if $as = 0$ for some $s \in S$ then $a/1 = 0/1$. Indeed $\ker \iota = \{a \in A | as = 0 \text{ some } s \in S\}$.