

Chapter 8

Commutative algebra

In case I forget, throughout the chapter *all rings are commutative*.

8.1 Localization revisited

First, I want to go back and look more closely at the localization construction, since this is a basic tool in commutative algebra. Let R be a commutative ring and $S \subseteq R$ be a multiplicative set. Recall the localization of R at S is a ring homomorphism

$$i_S : R \rightarrow S^{-1}R$$

such that $i_S(s)$ is a unit for each $s \in S$, and moreover given any other ring homomorphism $f : R \rightarrow R'$ such that $f(s)$ is a unit for each $s \in S$, there exists a unique ring homomorphism $\bar{f} : S^{-1}R \rightarrow R'$ such that $f = \bar{f} \circ i_S$. Of course, we have in mind the explicit construction for the ring $S^{-1}R$, so its elements are represented as r/s for $r \in R, s \in S$ and the map i_S is simply the map $r \mapsto r/1$.

We wish to understand in more detail the relationship between the lattice of ideals in R and in $S^{-1}R$. Let I be an ideal of R . Let

$$S^{-1}I = \{a/s \mid a \in I, s \in S\} \subseteq S^{-1}R.$$

You easily check that $S^{-1}I$ is an ideal of $S^{-1}R$. Thus, we have a map $I \mapsto S^{-1}I$ from ideals of R to ideals of $S^{-1}R$. This preserves containments of ideals and commutes with the basic operations on ideals such as:

$$\begin{aligned} S^{-1}(I + J) &= S^{-1}I + S^{-1}J, \\ S^{-1}(I \cap J) &= S^{-1}I \cap S^{-1}J, \\ S^{-1}(IJ) &= (S^{-1}I)(S^{-1}J) \end{aligned}$$

for all ideals I, J of R . On the other hand, there is a map from ideals of $S^{-1}R$ to ideals of R : take an ideal J of $S^{-1}R$ and consider its pre-image $i_S^{-1}(J)$ under the homomorphism $i_S : R \rightarrow S^{-1}R$. It is clearly an ideal in R .

8.1.1. Lemma. *Every ideal in $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I in R .*

Proof. Take an ideal J in $S^{-1}R$. Set $I = i_S^{-1}(J)$. We check that $J = S^{-1}I$. Well, every element of $S^{-1}I$ has the form $a/s = a/1 \cdot 1/s$ for $a \in R$ with $i_S(a) = a/1 \in J$, so $S^{-1}I \subseteq J$. On the other hand, take any element $a/s \in J$. Then, as $1/s$ is a unit in $S^{-1}R$, $a/1 \in J$ hence $a \in I$ hence $a/s \in S^{-1}I$. \square

Thus our map from ideals of R to ideals of $S^{-1}R$ is surjective. But it will certainly not be bijective in general: for instance if I is an ideal of R with $I \cap S \neq \emptyset$, then $S^{-1}I = S^{-1}R$.

8.1.2. Lemma. *Let $f : R \rightarrow R'$ be a homomorphism of commutative rings and P' be a prime ideal of R' . Then, $P := f^{-1}(P')$ is a prime ideal of R .*

Proof. Consider the map $g : R \rightarrow R'/P'$ obtained by composing f with the quotient map $R' \rightarrow R'/P'$. Its kernel is precisely the ideal $P = f^{-1}(P')$ of R . Hence, g factors to give a monomorphism $R/P \hookrightarrow R'/P'$. By the characterization of prime ideals, R'/P' is an integral domain. Hence, R/P is an integral domain too as it is isomorphic to a unital subring of R'/P' . Hence P is a prime ideal of R . \square

Prime ideals under localization. *The maps $I \mapsto S^{-1}I$ and $J \mapsto i_S^{-1}(J)$ give a 1-1 correspondence between the set of prime ideals of R that are disjoint from S and the set of prime ideals of $S^{-1}R$.*

Proof. Let P be a prime ideal in R with $S \cap P = \emptyset$. We first check that $S^{-1}P$ is a prime ideal in $S^{-1}R$. Well, if $S^{-1}P = S^{-1}R$, then we could write $1/1 \in S^{-1}R$ as p/s for some $p \in P, s \in S$. But that would give that $1/1 = p/s$, i.e. $(s-p)s' = 0$ for some $s' \in S$, so $ss' = ps' \in P$, contradicting disjointness of P and S . Now suppose $(a/s)(a'/s') \in S^{-1}P$. Then, $aa'/ss' = p/s''$ so that $aa's''t = pss't$ for some $t \in S$. But that implies $aa's''t \in P$, so since $S \cap P = \emptyset$ we have that one of $a, a' \in P$. Hence, one of (a/s) and (a'/s') is in $S^{-1}P$. So $S^{-1}P$ is prime.

Thus the map $P \mapsto S^{-1}P$ sends prime ideals disjoint from S to prime ideals of $S^{-1}R$. By Lemma 8.1.2, the map $J \mapsto i_S^{-1}(J)$ sends primes in $S^{-1}R$ to primes in R . We also showed in Lemma 8.1.1 that $S^{-1}(i_S^{-1}(J)) = J$ for any ideal J of $S^{-1}R$, so certainly $i_S^{-1}(J)$ is disjoint from S for any proper ideal J of $S^{-1}R$.

It therefore remains to show that $i_S^{-1}(S^{-1}P) = P$ if P is a prime ideal of R disjoint from S . Obviously, $P \subseteq i_S^{-1}(S^{-1}P)$. Finally, take $a \in i_S^{-1}(S^{-1}P)$. Then, $i_S(a) = a/1 = b/s$ for some $b \in P, s \in S$. So $ast = bt \in P$ for some $t \in S$. Hence $a \in P$. So, $P \supseteq i_S^{-1}(S^{-1}P)$. \square

Now we focus on the most important special case of localization. Let P be a prime ideal of R . Then, $S = R - P$ is a multiplicative set. We (confusingly) denote the localization $i_S : R \rightarrow S^{-1}R$ in this case by

$$i_P : R \rightarrow R_P$$

and call it the localization of R at prime ideal P . Moreover, for an ideal I of R , we denote the ideal $S^{-1}I$ of $S^{-1}R = R_P$ instead by I_P . Now let us restate the preceding theorem in this special case:

Prime ideals under localization'. *Let P be a prime ideal in R . Then, there is a 1-1 correspondence between the prime ideals of R contained in P and the prime ideals of R_P .*

This shows that in particular, R_P has a *unique* maximal ideal, namely, P_P . This property is so crucial in commutative algebra that we give it a special name: call a commutative ring R *local* if it has a unique maximal ideal. If R is a commutative local ring, with unique maximal ideal M , the quotient ring R/M (which is a field!) is called the *residue field* of R .

Examples. (1) The ring \mathbb{Z}_{p^n} of integers modulo p^n , p prime, is a commutative local ring with unique maximal ideal (p) . Note the proper ideals of \mathbb{Z}_{p^n} are

$$(1) \supset (p) \supset (p^2) \supset \cdots \supset (p^{n-1}) \supset (0),$$

i.e. the powers of the maximal ideal (p) . But this is not very interesting: it is just a quotient ring of the next example, and obviously any non-zero quotient of a local ring is again a local ring.

(2) Consider $R = \mathbb{Z}_{(p)}$ where p is prime, i.e. the ring \mathbb{Z} localized at the prime ideal (p) . So elements of $\mathbb{Z}_{(p)}$ look like m/n where $(p, n) = 1$. It is a commutative local ring (as it is obtained by localizing \mathbb{Z} at a prime ideal) with unique maximal ideal M consisting of all m/n such that $p|m$.

Note *all* proper ideals of $\mathbb{Z}_{(p)}$ are the ideals M^i for $i \geq 1$, and $M^i = \{m/n \mid (m, n) = 1, p^i \mid m\}$. This time,

$$R \supset M \supset M^2 \supset M^3 \supset \dots$$

is an infinite descending chain of ideals so R is not Artinian.

8.2 Completion

Now I want to explain another important construction in commutative algebra. Actually, we will not go far enough to see the true significance of the construction, but you need to be aware of the two main examples discussed below...

To start with, let R be any commutative ring. Write $R[[X]]$ for the set of *all* sequences (a_0, a_1, a_2, \dots) with $a_i \in R$. Define addition coordinatewise and (commutative) multiplication by convolution

$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots) \quad \text{where} \quad c_n = \sum_{i+j=n} a_i b_j.$$

Elements of $R[[X]]$ are called *formal power series* and the notation

$$\sum_{i=0}^{\infty} a_i X^i$$

is used as a suggestive notation for the element (a_0, a_1, \dots) . Note $R[[X]]$ contains the polynomial ring $R[X]$ as a subring, namely, the subring consisting of all (a_0, a_1, \dots) with all but finitely many a_i being zero.

Units in the ring of formal power series. A formal power series $\sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ is a unit if and only if a_0 is a unit in R .

Proof. The forward implication is easy, so I leave it to you. Conversely, suppose that a_0 is a unit. Define $b_0, b_1, b_2, \dots \in R$ inductively by setting

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_1 &= a_0^{-1}(-a_1 b_0), \dots, \\ b_n &= a_0^{-1}(-a_1 b_{n-1} - \dots - a_n b_0). \end{aligned}$$

Then, $\sum_{i=0}^{\infty} b_i X^i$ is a two-sided inverse for $\sum_{i=0}^{\infty} a_i X^i$. \square

Now suppose that R is in fact a field F . Then I claim that $F[[X]]$ is actually a local ring with unique maximal ideal being (X) , the ideal consisting of all formal power series with constant term being zero. Well, by the description of units in $F[[X]]$, (X) is (miraculously) the set of all non-units in the ring $F[[X]]$. If I is a proper ideal of $F[[X]]$, then I contains no units, so $I \subseteq (X)$. Hence (X) is the unique maximal ideal.

The ring of formal power series actually arises as a special case of a general construction known as *completion* (there is a formal reason for the name but we will not go into it here). To describe the construction in general, let R be a local ring with unique maximal ideal M . There is an obvious map

$$\pi_n : R/M^n \rightarrow R/M^{n-1}$$

for each $n \geq 1$. Define \bar{R} , the *completion of the local ring* R , to be the subring of

$$\prod_{n \geq 1} R/M^n$$

consisting of all tuples $(f_n)_{n \geq 1}$ such that $\pi_n(f_n) = f_{n-1}$ for each $n > 1$. There is a canonical homomorphism

$$\pi : R \rightarrow \bar{R}$$

mapping $a \in R$ to the element $(f_n)_{n \geq 1}$ of \bar{R} with f_n being the image of a under the quotient map $R \rightarrow R/M^n$ for each $n \geq 1$.

We remark that if $M^n = (0)$ for some $n \geq 1$ (which is the case if R is Artinian), then the map $\pi : R \rightarrow \bar{R}$ is actually an isomorphism. So completion is really not at all interesting in this case!! Indeed, if $M^n = (0)$, define a map $j : \bar{R} \rightarrow R$ by mapping $(f_n)_{n \geq 1} \in \bar{R}$ to $f_n \in R/M^n = R$. You can check that this is a two-sided inverse to π .

Now is a good time to recall the notion of *Noetherian ring* from section 5.2. The best results in commutative algebra tend to be concerned only with the case of commutative Noetherian rings! For instance:

Krull's intersection theorem. *Let R be a commutative Noetherian ring and I be an ideal of R . Let M be a finitely generated R -module and $N = \bigcap_{n \geq 1} (I^n M)$. Then, $IN = N$.*

Eeek!! The first time I attempted to understand this theorem I made the fundamental error. You need to understand why it is not *obvious* that $IN = N$... The point is that given two submodules A and B , it is not the case that $I(A \cap B) = (IA) \cap (IB)$. Obviously, the left hand side is contained in the right. But something in the right hand side is of the form $\sum x_i a_i = \sum y_j b_j$ for $x_i, y_j \in I, a_i \in A, b_j \in B$. There is no reason you should be able to write this as $\sum z_k c_k$ for $z_k \in I, c_k \in A \cap B$.

Proof. (after Hungerford, VIII.4, exercises 1 and 2).

Step zero. Let \mathcal{A} be the set of all R -submodules S of M with the property that $N \cap S = IN$. Note \mathcal{A} is non-empty since $IN \in \mathcal{A}$. Then a routine Zorn's lemma argument gives that \mathcal{A} possesses a maximal element, U say.

Step one. Fix $a \in I$. We show that there exists an integer m (depending on a) such that $a^m M \subseteq U$.

To see this, let

$$D_k = \{x \in M \mid a^k x \in U\}.$$

Then, $D_0 \subseteq D_1 \subseteq \dots$ is an ascending chain of R -submodules of M , so stabilizes since M is Noetherian (Theorem 5.2.2). Say $D_m = D_{m+1} = \dots$. Now consider

$$N \cap (a^m M + U).$$

It obviously contains $N \cap U = IN$. On the other hand, take any element $a^m x + u$ of $N \cap (a^m M + U)$ not in $IN = N \cap U$. Then $a^m x$ is not an element of U , so $x \notin D_m$. But $a^{m+1} x + au \in IN = N \cap U$, so that $a^{m+1} x$ is in U . This implies that $x \in D_{m+1}$ which is a contradiction since $D_m = D_{m+1}$. This shows that

$$N \cap (a^m M + U) = IN.$$

Hence, by maximality of U , $a^m M + U = U$, i.e. $a^m M \subseteq U$ as required.

Step two. We show that there exists an integer m such that $I^m M \subseteq U$.

Well, since R is Noetherian, I is finitely generated, say by a_1, \dots, a_r . By step one, there are (possibly different) integers m_1, \dots, m_r such that $a_i^{m_i} M \subseteq U$. Let $m = m_1 + \dots + m_r$. Then, I claim that $a^m M \subseteq U$ for all $a \in I$. Indeed, take any element of I^m . It looks like an R -linear combination of monomials each of degree at least m in the a_i . A monomial of degree m in the a_i must involve some a_i at least m_i times. By assumption, $a_i^{m_i} M \subseteq U$. Hence $a^m M \subseteq U$.

Step three. Now we complete the proof. By step two, there exists an integer m such that $I^m M \subseteq U$. Then, $N = N \cap I^m M \subseteq N \cap U = IN$. This shows that $N \subseteq IN$, while obviously $IN \subseteq N$. Hence $N = IN$ as required. \square

8.2.1. Corollary. *If R is a commutative Noetherian ring, then $\bigcap_{n \geq 1} J(R)^n = (0)$.*

Proof. Let $J = J(R)$. We have that $M = \bigcap_{n \geq 1} J^n$ is an ideal of R , hence a finitely generated R -module since R is Noetherian and Corollary 5.2.4. By Krull's intersection theorem, $JM = M$. So $M = (0)$ by Nakayama's lemma. \square

This is an important result in the theory of completions, for it gives us:

Injectivity of completion. *If R is a Noetherian local ring, then the canonical map $\pi : R \rightarrow \bar{R}$ is injective.*

Proof. For a commutative ring, its Jacobson radical is the intersection of *all* maximal ideals of R . So in case R is a commutative local ring, its Jacobson radical is exactly its unique maximal ideal M . By Corollary 8.2.1 and the Noetherian hypothesis, $\bigcap_{n \geq 1} M^n = (0)$. Now, if $\pi(a) = 0$ for $a \in R$, then $a + M^n = M^n$ for each $n \geq 1$, i.e. $a \in \bigcap_{n \geq 1} M^n$. Hence $a = 0$. \square

Now let R be a *Noetherian integral domain*. Let P be a prime ideal of R . Then, the localization $i_P : R \rightarrow R_P$ is injective. Moreover, the local ring R_P is Noetherian (exercise!), so by the theorem, the canonical map $\pi : R_P \rightarrow \bar{R}_P$ is injective. Composing, we thus obtain an embedding of R into its *completion \bar{R}_P at the prime ideal P* .

Example one. Let F be a field. Then, the ring $F[[X]]$ of formal power series over F is (isomorphic to) the completion of the polynomial ring $F[X]$ at the prime ideal (X) .

Proof. Let $R = F[X]_{(X)}$, the localization of the polynomial ring $F[X]$ at the prime ideal (X) . Let M be the unique maximal ideal of R . Then, M^n consists of rational functions of the form $f(X)/g(X)$ where $g(X)$ has non-zero constant term and $X^n | f(X)$. The quotient ring R/M^n is isomorphic to

$$F[X]/(X^n),$$

so consists of "truncated polynomials".

Now, an element of the completion \bar{R} looks like a tuple $(f_n)_{n \geq 1}$ of polynomials $f_n \in F[X]/(X^n)$ with $\pi_n(f_n) = f_{n-1}$. We can represent f_n as $a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + M^n$ for unique $a_0, a_1, \dots, a_{n-1} \in F$. The condition $\pi_n(f_n) = f_{n-1}$ means that *all* f_m for $m \geq n$ have the same leading coefficients a_0, \dots, a_{n-1} as f_n when represented in this way. So there is a uniquely determined infinite tuple $(a_0, a_1, a_2, a_3, \dots)$ of elements of F , i.e. an element of $F[[X]]$, such that $f_n = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + M^n$ for each $n \geq 1$. We get in this way the required isomorphism between \bar{R} and $F[[X]]$. \square

Example two. The second important example of completion is *the completion of \mathbb{Z} at a maximal ideal (p)* . To explain this, recall a basic fact about integers. Let p be a prime. Then any integer $n \geq 0$ can be written as

$$n = b_0 + b_1p + \cdots + b_r p^r$$

for unique $0 \leq b_i < p$ and some sufficiently large r . This is called the *p -adic expansion of n* .

Now let $R = \mathbb{Z}_{(p)}$ with unique maximal ideal $M = (p)$. Then, $M^n = (p^n)$ and $R/M^n \cong \mathbb{Z}_p^n$. An element of the completion \bar{R} is thus an infinite series (a_1, a_2, \dots) with $a_i \in \mathbb{Z}_p^i$, such that $a_n \equiv a_{n-1} \pmod{p^{n-1}}$ for each $n > 1$. Now, we can write a_n as $\bar{a}_n + (p^n)$ for a unique $0 \leq \bar{a}_n < p^n$. Then let

$$\bar{a}_n = b_0 + b_1p + \cdots + b_{n-1}p^{n-1}$$

be the p -adic expansion of \bar{a}_n , so $0 \leq b_i < p$ for each i . The condition $a_n \equiv a_{n-1} \pmod{p^{n-1}}$ for each $n > 1$ simply means that for all $m > n$, the leading b_i when a_m is written in this form agree with the ones arising for a_n . In other words, an element of \bar{R} looks like an *infinite p -adic expansion*. You should compare all this carefully with the two constructions of formal power series $F[[X]]$ above!!!

The ring we have just constructed – the completion $\bar{\mathbb{Z}}_{(p)}$ of the local ring $\mathbb{Z}_{(p)}$ – is a very important example of a local ring. It is called the *ring of p -adic integers*, usually denoted \mathbb{Z}_p which

is very unfortunate for us since we have been using \mathbb{Z}_p to denote $\mathbb{Z}/(p)$. (Really, \mathbb{Z}_p should be reserved for p -adic integers and one should write $\mathbb{Z}/(n)$ for integers modulo n !!!). The residue field of the p -adic integers \mathbb{Z}_p is the field $\mathbb{Z}/(p)$ of characteristic p , and the field of fractions of \mathbb{Z}_p is denoted \mathbb{Q}_p and is of characteristic 0.

8.3 The prime spectrum of a ring

Let R be a commutative ring.

8.3.1. Lemma. *Let I be an ideal of R and S be a multiplicative set with $S \cap I = \emptyset$. Then, the set of all ideals of R disjoint from S and containing I has a maximal element. Any such maximal element P is prime.*

Proof. Let \mathcal{A} be the set of all ideals of R disjoint from S and containing I . It is non-empty since $I \in \mathcal{A}$. Now a routine Zorn's lemma argument gives that \mathcal{A} has a maximal element P , certainly a proper ideal of R .

To see that P is prime, suppose for a contradiction that we can find ideals A, B of R such that $AB \subseteq P$ but $A \not\subseteq P, B \not\subseteq P$. Then, $A + P$ is strictly larger than P , so meets S by maximality, and similarly $B + P$ meets S . So we can find $p_1, p_2 \in P, a \in A, b \in B$ and $s_1, s_2 \in S$ such that $p_1 + a = s_1, p_2 + b = s_2$. Then,

$$s_1 s_2 = p_1 p_2 + p_1 b + a p_2 + ab \in P + AB \subseteq P.$$

This is a contradiction since S is disjoint from P . \square

If I is an ideal of R , its *radical* is by definition

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0\}.$$

Characterization of radicals of ideals. *For a proper ideal I of R , \sqrt{I} is the intersection of all prime ideals of R containing I .*

Proof. Let J be the intersection of all prime ideals of R containing I . Take $a \in R$ such that $a^n \in I$ for some $n > 0$. Then, for any prime ideal P containing I , $a^n \in P$ so $a \in P$. Hence, a lies in each prime ideal containing I , so a lies in J . So $\sqrt{I} \subseteq J$.

Conversely, suppose we have $a \in R - \sqrt{I}$, so $a^n \notin I$ for any $n > 0$. Let $S = \{a^n + x \mid n > 0, x \in I\} \cup \{1\}$, a multiplicative set disjoint from I . Applying Lemma 8.3.1, we can find a prime ideal P of R containing I and disjoint from S . Now, $a \notin P$ so as P contains J , $a \notin J$, so $R - \sqrt{I} \subseteq R - J$. In other words, $J \subseteq \sqrt{I}$. \square

Now let $\text{Spec } R$ denote the set of all prime ideals of R . We introduce a topology on $\text{Spec } R$, called the *Zariski topology*, by defining the closed sets. Let I be an ideal of R . Define

$$V(I) = \{P \in \text{Spec } R \mid P \supseteq I\}.$$

Then the $V(I)$ as I runs over all ideals of R are precisely the closed sets of $\text{Spec } R$. We check that these do indeed define the closed sets of a topology:

Zariski topology. *Let R be a commutative ring.*

- (i) *For ideals I, J of R , $V(I) \cup V(J) = V(IJ)$.*
- (ii) *Give a family of ideals $\{I_\omega\}_{\omega \in \Omega}$, $\bigcap_{\omega \in \Omega} V(I_\omega) = V(\sum_{\omega \in \Omega} I_\omega)$.*
- (iii) *$V(I) \subseteq V(J)$ if and only if $\sqrt{I} \supseteq \sqrt{J}$.*

(Note (iii) shows in particular that the correspondence $I \mapsto V(I)$ between ideals of R and closed sets in $\text{Spec } R$ is *inclusion reversing*.)

Proof. (i) If P is a prime ideal of R containing either I or J clearly P contains IJ . Hence $V(I) \cup V(J) \subseteq V(IJ)$. And if P contains IJ then since P is prime, P contains one of I or J , hence $V(IJ) \subseteq V(I) \cup V(J)$.

(ii) If P is an element of the left hand side, then P contains all I_ω , hence contains $\sum_{\omega \in \Omega} I_\omega$ so is an element of the right hand side. And if P contains $\sum_{\omega \in \Omega} I_\omega$, then in particular P contains I_ω hence lies in $V(I_\omega)$ for each ω , so P lies in the intersection of the $V(I_\omega)$'s.

(iii) If $V(I) \subseteq V(J)$, then every prime ideal of R that contains I also contains J . Hence, $\sqrt{I} \supseteq \sqrt{J}$ by the characterization of radicals of ideals. Conversely, suppose $\sqrt{I} \supseteq \sqrt{J}$. Let P be a prime ideal containing I . We need to show that P also contains J : $P \supseteq \sqrt{I} \supseteq \sqrt{J} \supseteq J$. \square

Now suppose $\phi : R \rightarrow R'$ is a ring homomorphism. We have seen Lemma 8.1.2 that if P' is a prime ideal of R' , i.e. a point in $\text{Spec } R'$, then $\phi^{-1}(P')$ is a prime ideal of R , i.e. a point in $\text{Spec } R$. Thus we get from ϕ a map

$$\text{Spec } \phi : \text{Spec } R' \rightarrow \text{Spec } R, \quad P' \mapsto \phi^{-1}(P').$$

This is actually a *continuous map* for the Zariski topologies! Indeed, if $V(I)$ is a closed set in $\text{Spec } R$, for I an ideal of R , then $(\text{Spec } \phi)^{-1}(V(I)) = V(J)$ where J is the ideal of R' generated by $\phi(I)$ (it is a good exercise to check this for yourself). If you like (rather a useless statement), this shows that Spec is a contravariant functor from the category of commutative rings to the category of topological spaces.

But be warned: the Zariski topology is a rather weird topology! So basic notions useful in analysis and topology (e.g. completeness) are really not that useful to us – rather, the introduction of the Zariski topology is just to give us the beautiful *language* of open and closed sets

To illustrate how unpleasant the Zariski topology is, first note that *not all points are closed*. Indeed, if P is a prime ideal of R and $\{P\}$ is a closed set in the Zariski topology, then

$$\{P\} = V(I)$$

for some ideal I of R . So $P \supseteq I$ and I is contained in no other prime ideal of R . In particular, P is a *maximal ideal*. On the other hand, clearly if P is a maximal ideal of R , then $\{P\} = V(P)$ so is closed. We have shown:

8.3.2. Lemma. *The point $P \in \text{Spec } R$ is a closed point if and only if P is a maximal ideal of R .*

Continuing the weirdness of the Zariski topology, the open sets in the Zariski topology are rather large! For instance the topology is not in general Hausdorff – so all your usual intuition about well separated topological spaces really do not apply!

Consider for an example now $R = \mathbb{Z}$. Then, $\text{Spec } R$ can be identified with the set of all primes, which are closed points, together with zero, which is not a closed point – indeed its closure is *all* of $\text{Spec } R$. The closed sets of $\text{Spec } R$ are:

- (1) The empty set (which equals $V(R)$);
- (2) All of $\text{Spec } R$ (which equals $V((0))$);
- (3) Any finite set of primes (this being $V((n))$ where n is the product of those primes).

I will say more about the Zariski topology in section 8.6 – first, we need to develop a little more machinery to understand it better. But hopefully the thought that there is a topological space attached to a ring, the points of which are the prime ideals, helps to explain some of the language like “localization” and “local rings”. Indeed, the local ring R_P of R at the prime ideal P really corresponds (morally at least) to focusing attention locally on the point P . The idea is that many global properties of the ring R can be detected by studying local properties of *all* local rings R_P for all prime ideals P of R .

8.4 Ring extensions

Let R be a commutative ring. We say $R \subseteq S$ is a *ring extension* if S is another commutative ring and R is a unital subring of S . For example, if R is an integral domain and S is its field of fractions, then we obtain a ring extension $R \subseteq S$ by viewing R as a subring of S via the canonical embedding $i : R \rightarrow S$. Of course, any *field extension* is in the first place a ring extension, so our study of ring extensions should generalize the earlier study of field extensions.

If $R \subseteq S$ is a ring extension and A is a subset of S , the notation $R[A]$ will denote the smallest unital *subring* of S generated by R and A . Thus elements of $R[A]$ look like polynomials in the elements of A with coefficients of R . It is very important not to confuse the subring $R[A]$ with the R -submodule of S generated by A . Whenever you see the word “generate” in algebra you need to make sure you know whether it means as a ring or as a module...

In case $S = R[a_1, \dots, a_n]$ for finitely many elements $a_i \in S$, S is called a *finitely generated R -algebra*. But it may or may not be finitely generated as an R -module.

8.4.1. Lemma. *Let $R \subseteq S \subseteq T$ be ring extensions such that T is a finitely generated S -module and S is a finitely generated R -module. Then, T is a finitely generated R -module.*

Proof. Say S is generated by s_1, \dots, s_n as an R -module, and T is generated by t_1, \dots, t_m as an S -module. I claim that $\{s_i t_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ generate T as an R -module. Take any $t \in T$. We can write it as

$$t = \sum_{j=1}^m a_j t_j$$

for $a_j \in S$. Then each a_j can be expanded in terms of the s_i to get that

$$t = \sum_{i=1}^n \sum_{j=1}^m b_{i,j} s_i t_j$$

for some $b_{i,j} \in R$. Hence the $s_i t_j$ do indeed generate T as an R -module. \square

The key idea when studying ring extensions is that of an *integral extension*. Let $R \subseteq S$ be a ring extension and $s \in S$. If there exists a *monic* polynomial $f(X) \in R[X]$ such that $f(s) = 0$, then s is called *integral over R* . If every $s \in S$ is integral over R , then $R \subseteq S$ is called an *integral extension*.

For examples:

(1) A *field extension* $E \subseteq F$ is an integral extension as just defined if and only if it is an algebraic extension in the old sense.

(2) Consider the ring extension $\mathbb{Z} \subseteq \mathbb{R}$. Then, $\mathbb{Z} \subseteq \mathbb{Z}[\frac{1}{\sqrt{3}}]$ is *not* an integral extension. For $\frac{1}{\sqrt{3}}$ has minimal polynomial $3X^2 - 1$. Now if $\frac{1}{\sqrt{3}}$ is integral over \mathbb{Z} , it is a root of a monic polynomial, $f(X)$ say. Then, $3X^2 - 1$ divides $f(X)$ in $\mathbb{Q}[X]$. So, since the leading coefficient of $f(X)$ is a unit in \mathbb{Z} , the division algorithm for polynomials (section 2.3) implies that $3X^2 - 1$ also divides $f(X)$ in $\mathbb{Z}[X]$, which is impossible since 3 is not a unit in \mathbb{Z} !!!

Now we need a rather technical theorem:

Characterization of integral elements. *Let $R \subseteq S$ be a ring extension and $s \in S$. The following are equivalent:*

- (i) s is integral over R ;
- (ii) $R[s]$ is a finitely generated R -module;
- (iii) there is a unital subring T of S containing $R[s]$ with T being finitely generated as an R -module;
- (iv) there is an $R[s]$ -submodule U of S which is finitely generated as an R -module and whose annihilator in $R[s]$ is zero.

Proof. (i) \Rightarrow (ii). Suppose s is a root of the monic polynomial $f(X) \in R[X]$ of degree n . Every element of $R[s]$ is of the form $g(s)$ for some polynomial $g(X) \in R[X]$. By the division algorithm for polynomials,

$$g(X) = f(X)q(X) + r(X)$$

where $\deg r < \deg f = n$. Hence,

$$g(s) = r(s)$$

so every element of $R[s]$ is of the form $g(s)$ for some polynomial $g(X) \in R[X]$ of degree $< n$. This shows every element of $R[s]$ is an R -linear combination of $1, s, \dots, s^{n-1}$, i.e. $R[s]$ is finitely generated as an R -module.

(ii) \Rightarrow (iii). Take $T = R[s]$.

(iii) \Rightarrow (iv). Take $U = T$. Since $R \subseteq R[s] \subseteq T$, U is an $R[s]$ -module which is finitely generated as an R -module by assumption. We need to show that the annihilator of U in $R[s]$ is zero. Well, since $1 \in U$, $aU = 0$ for $a \in R[s]$ implies $a = a1 = 0$.

(iv) \Rightarrow (i). Let U be an $R[s]$ -submodule of S that is generated as an R -module by u_1, \dots, u_n . Note $su_i \in U$ for each i . Therefore, there exist $r_{i,j} \in R$ such that

$$\begin{aligned} su_1 &= r_{1,1}u_1 + \cdots + r_{1,n}u_n \\ su_2 &= r_{2,1}u_1 + \cdots + r_{2,n}u_n \\ &\vdots \\ su_n &= r_{n,1}u_1 + \cdots + r_{n,n}u_n. \end{aligned}$$

Hence,

$$\begin{aligned} (r_{1,1} - s)u_1 + r_{1,2}u_2 + \cdots + r_{1,n}u_n &= 0 \\ r_{2,1}u_1 + (r_{2,2} - s)u_2 + \cdots + r_{2,n}u_n &= 0 \\ &\vdots \\ r_{n,1}u_1 + r_{n,2}u_2 + \cdots + (r_{n,n} - s)u_n &= 0. \end{aligned}$$

Let M be the $n \times n$ matrix with i, j -entry equal to $(r_{i,j})$ for $i \neq j$ and $r_{i,i} - s$ on the diagonal.

I claim that $(\det M)u_i = 0$ for each $i = 1, \dots, n$. Indeed, consider the matrix

$$U_i = \text{diag}(1, \dots, 1, u_i, 1, \dots, 1)$$

where u_i appears in the i th diagonal entry. Then,

$$(\det M)u_i = \det M \det U_i = \det(MU_i).$$

So I just need to show that $\det(MU_i) = 0$. Let M' be the matrix obtained from MU_i by adding u_j times the j th column of MU_i to the i th column for each $j \neq i$. Then, $\det M' = \det(MU_i)$. Moreover, the k th entry of M' is

$$m_{k,1}u_1 + \cdots + m_{k,i}u_i + \cdots + m_{k,n}u_n = 0.$$

So the i th column of M' is zero, so $\det M' = 0$ as claimed.

This shows that if $D \in R[s]$ denotes the determinant of M , we have that $Du_i = 0$ for each $i = 1, \dots, n$. Hence, since the u_i generate U as an R -module, $DU = 0$. But by assumption the annihilator of U in $R[s]$ is zero, hence $D = 0$.

Now consider finally the matrix P with ij -entry equal to $-r_{i,j}$ for $i \neq j$ and $X - r_{i,i}$ on the diagonal. Then, $\det P \in R[X]$ is a monic polynomial, and we have just shown that s is a zero of $\det P$. Therefore, s is integral over R . \square

8.4.2. Corollary. *Let $R \subseteq S$ be a ring extension such that S is finitely generated as an R -module. Then, $R \subseteq S$ is an integral extension.*

Proof. Take $s \in S$ and let $T = S$ in part (iii) of the above characterization, to get that s is integral over R . \square

8.4.3. Corollary. *If $R \subseteq S$ is a ring extension and $s_1, \dots, s_t \in S$ are integral over R , then $R[s_1, \dots, s_t]$ is a finitely generated R -module and $R \subseteq R[s_1, \dots, s_t]$ is an integral ring extension.*

Proof. We have a tower of ring extensions

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \dots, s_t].$$

For each i , s_i is integral over R hence integral over $R[s_1, \dots, s_{i-1}]$.

Hence, $R[s_1, \dots, s_i]$ is a finitely generated $R[s_1, \dots, s_{i-1}]$ -module by the above characterization. By induction on i , $R[s_1, \dots, s_{i-1}]$ is a finitely generated R -module. Hence by Lemma 8.4.1, $R[s_1, \dots, s_i]$ is a finitely generated R -module. Hence it is integral by Corollary 8.4.2. \square

Now we can prove the following generalization of Corollary 7.1.3:

Transitivity of integral extensions. *Let $R \subseteq S$ and $S \subseteq T$ be integral extensions. Then, $R \subseteq T$ is also an integral extension.*

Proof. Take $t \in T$. Then, t is integral over S so the root of some monic polynomial $f(X) \in S[X]$. Say $f(X) = X^n + s_{n-1}X^{n-1} + \cdots + s_0$. Note $f(X) \in R[s_0, \dots, s_{n-1}][X]$, so t is actually integral over $R[s_0, \dots, s_{n-1}]$. This is an integral extension of R that is finitely generated as an R -module by Corollary 8.4.3. Hence by Lemma 8.4.1, $R[s_0, \dots, s_{n-1}, t]$ is a finitely generated R -module. Now finally using (iii) of the characterization of integral elements and the fact that $R[t]$ is contained in $R[s_0, \dots, s_{n-1}, t]$, we get that t is integral over R . \square

Having introduced integral extensions, we should mention the notion of the *integral closure* of a ring extension. To start with we have:

Existence of integral closures. *Let $R \subseteq S$ be a ring extension and \hat{R} be the set of all elements of S which are integral over R . Then, \hat{R} is an integral extension of R .*

Proof. Let $s, t \in \hat{R}$. Since s, t are integral over R , so is $R[s, t]$. So, $R[s, t] \subseteq \hat{R}$. In particular, st and $s - t$ are both in \hat{R} , so \hat{R} is a ring extension of R . \square

If $R \subseteq S$ is a ring extension, the subring \hat{R} of S is called the *integral closure of R in S* . Note despite the notation, the integral closure \hat{R} depends *both* on R and on S !!! In case $R = \hat{R}$, one says that R is *integrally closed in S* .

For example, the ring \mathbb{Z} is integrally closed in its field of fractions. Indeed, we need to show that every $a/b \in \mathbb{Q}$ which is integral over \mathbb{Z} is actually in \mathbb{Z} . Well, take $a/b \in \mathbb{Q}$ with $(a, b) = 1$ and suppose that a/b is a root of

$$X^n - c_{n-1}X^{n-1} - \cdots - c_1X - c_0.$$

Substituting a/b and multiplying through by b^{n-1} , we get that

$$a^n/b = c_{n-1}a^{n-1} + c_{n-2}a^{n-2}b + \cdots + c_0b^{n-1}.$$

The right hand side is an integer, hence the left hand side is, hence b divides a^n . Since $(a, b) = 1$, this implies that $b = 1$ and $a/b \in \mathbb{Z}$ as required.

You can show with a similar argument that *any unique factorization domain is integrally closed in its field of fractions*. For instance, the polynomial ring $F[X_1, \dots, X_n]$ for F a field is integrally closed in its field of fractions $F(X_1, \dots, X_n)$.

For another example, consider \mathbb{Z} , which we have just seen is integrally closed in \mathbb{Q} . However, \mathbb{Z} is *not* integrally closed in \mathbb{C} : $i \in \mathbb{C}$ is integral over \mathbb{Z} but is not an element of \mathbb{Z} .

The following lemma will be needed in section 8.6.

8.4.4. Lemma. *Let $R \subseteq S$ be an integral extension and assume that S is an integral domain. Then, R is a field if and only if S is a field.*

Proof. Suppose R is a field. Take $0 \neq y \in S$. Then, y satisfies an equation

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$

with $a_i \in R$. Since S is an integral domain, we may assume that $a_n \neq 0$, hence $a_n^{-1} \in R$. Then,

$$y^{-1} = -a_n^{-1}(y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}) \in S.$$

Hence, S is a field.

Conversely, if S is a field, take $0 \neq x \in R$. Then, $x^{-1} \in S$, so we have an equation

$$x^{-m} + c_1 x^{1-m} + \cdots + c_m = 0$$

for $c_i \in R$. So

$$x^{-1} = -(c_1 + c_2 x + \cdots + c_m x^{m-1})$$

which is in R . \square

8.5 Hilbert's basis theorem

The remainder of the chapter is devoted to studying the structure of commutative Noetherian rings. First, we need a source of examples!

But let me warn you before we go any further of a potential source of confusion. Let R be a commutative ring. If I say that R is a *finitely generated ring* I mean that there are finitely many elements $r_1, \dots, r_n \in R$ such that every element of R can be written as a \mathbb{Z} -linear combination of monomials in the r_i . On the other hand, if I is an ideal of R , we have called I finitely generated if $I = (a_1, \dots, a_n)$ for some $a_i \in R$, that is, every element of I can be written as an R -linear combination of the a_i . Thus for instance, R is always finitely generated as an ideal (by 1), but may or may not be as a ring!! Whenever you see the words *finitely generated* in algebra, you should always think "what as", e.g. does it mean finitely generated as a ring or as a module (ideal).

Slightly more generally, if A is a commutative R -algebra, I say that A is a *finitely generated R -algebra* if there are finitely many elements $a_1, \dots, a_n \in A$ such that every element of A can be written as an R -linear combination of monomials in the a_i . Finitely generated algebras are very common in commutative algebra:

8.5.1. Lemma. *Suppose R is a commutative ring and A is a finitely generated commutative R -algebra. Then, A is a quotient of the polynomial algebra $R[X_1, \dots, X_n]$ for some $n \geq 1$.*

Proof. Say x_1, \dots, x_n generate A as an R -algebra. The map $X_i \mapsto x_i$ extends by the universal property of the polynomial algebra (a.k.a. the universal property of the symmetric algebra in section 6.5) to a unique R -linear ring homomorphism $R[X_1, \dots, X_n] \rightarrow A$. This is surjective since the x_i generate A . \square

This focuses our attention right away on the polynomial ring in finitely many indeterminates. The next result is absolutely fundamental as a result:

Hilbert basis theorem. *Let R be a commutative Noetherian ring (for example, a PID). Then the polynomial ring $R[X_1, \dots, X_n]$ in finitely many indeterminates is also Noetherian.*

Proof. By induction, it suffices to show just that $R[X]$ is Noetherian. Take an ideal J of $R[X]$. In view of the characterization of commutative Noetherian rings, we just need to show that J is finitely generated.

For $n \geq 0$, let I_n be the set of all $r \in R$ such that either $r = 0$ or r is the top coefficient of a polynomial $f \in J$ of degree n . Then, I_n is an ideal of R . Moreover, given $0 \neq r \in I_n$, r is the top coefficient of some polynomial $f \in J$ of degree n . So r is also the top coefficient of the polynomial Xf of degree $n + 1$, hence $r \in I_{n+1}$. This shows that

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

Hence since R is Noetherian, there exists $t \geq 0$ such that $I_n = I_t$ for all $n \geq t$.

Now, each I_s is finitely generated, say by $r_{s,1}, \dots, r_{s,n_s}$. Let $f_{s,j} \in J$ be a polynomial of degree s such that $r_{s,j}$ is the top coefficient of $f_{s,j}$. We will show that J is generated by the polynomials

$$\Omega = \{f_{s,j} \mid 0 \leq s \leq t, 1 \leq j \leq n_s\}.$$

Well, clearly, $(\Omega) \subseteq J$. Conversely, we show by induction on s that (Ω) contains all polynomials in J of degree $\leq s$. The case $s = 0$ is immediate since the polynomials in J of degree 0 are precisely the elements of I_0 .

For the induction step, take $g \in J$ of degree $s > 0$ with top coefficient r .

Case one: $s \leq t$. If $s \leq t$, then $r \in I_s$. So $r = a_1 r_{s,1} + \dots + a_{n_s} r_{s,n_s}$ for some $a_j \in R$. Then $f = a_1 f_{s,1} + \dots + a_{n_s} f_{s,n_s} \in (\Omega)$ has top coefficient r and degree s . So $g - f$ is in J and has degree $< s$, so lies in (Ω) by the induction hypothesis. Hence $g \in (\Omega)$ too.

Case two: $s > t$. Then $r \in I_s = I_t$ so $r = a_1 r_{t,1} + \dots + a_{n_t} r_{t,n_t}$ for some $a_j \in R$. Now

$$\sum_{j=1}^{n_t} a_j X^{s-t} f_{t,n_t} \in (\Omega)$$

and

$$g - \sum_{j=1}^{n_t} a_j X^{s-t} f_{t,n_t} \in J$$

has degree at most $s - 1$, so lies in (Ω) by the induction hypothesis. Hence $g \in \Omega$ too. \square

8.5.2. Corollary. *Suppose that R is a commutative Noetherian ring and A is a finitely generated R -algebra. Then, A is Noetherian.*

Proof. By Lemma 8.5.1, A is a quotient of $R[X_1, \dots, X_n]$ for some n . By the Hilbert basis theorem, $R[X_1, \dots, X_n]$ is Noetherian. So A is too by the lattice isomorphism theorem. \square

So now you can construct *very many* Noetherian commutative algebras – by generators and relations. Just start with a commutative Noetherian ring R (e.g. a field) and the polynomial ring $R[X_1, \dots, X_n]$ in finitely many indeterminates. Then, for any ideal I of $R[X_1, \dots, X_n]$ (generated by your choice of finitely many polynomials in the X_i), the quotient ring $R[X_1, \dots, X_n]/I$ is a finitely generated R -algebra, hence Noetherian.

8.6 Nullstellensatz

Now we specialize to considering *finitely generated integral domains over fields*. There are two extremes: on the one hand we have the polynomial ring $F[X_1, \dots, X_n]$ (in which the generators X_1, \dots, X_n are algebraically independent over F), on the other we have the *integral extensions* of F . Just as any field extension could be viewed as an algebraic extension of a purely transcendental extension, we can view an arbitrary finitely generated integral domain over a field as an integral extension of a polynomial algebra:

Noether's normalization lemma. *Let R be an integral domain which is finitely generated F -algebra. Then, there exists an algebraically independent subset t_1, \dots, t_r of R such that R is an integral extension of $F[t_1, \dots, t_r]$.*

Proof. Let $R = F[u_1, \dots, u_n]$. If $\{u_1, \dots, u_n\}$ is algebraically independent over F , the theorem is trivially true. Else, $\{u_1, \dots, u_n\}$ is algebraically dependent over F , so we can find a polynomial relation

$$f(u_1, \dots, u_n) = 0$$

between them, for some polynomial $f(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$. Reordering, we may assume that some monomial appearing in f involves X_1 .

Fix $r \geq 1$ and write

$$z_i = u_i - u_1^{r^{i-1}}.$$

We will show that r can be chosen so that u_1 is integral over $F[z_2, \dots, z_n]$. Before we do this, let us understand how the theorem follows. Well, then by induction on n there exists an algebraically independent subset t_1, \dots, t_r of $F[v_2, \dots, v_n]$ such that $F[v_2, \dots, v_n]$ is integral over $F[t_1, \dots, t_r]$. Then by transitivity of integral extensions, $R = F[u_1, v_2, \dots, v_n]$ is also integral over $F[t_1, \dots, t_r]$ as required.

It remains to show how to choose r . Let

$$g(X) = f(X, z_2 + X^r, z_3 + X^{r^2}, \dots, z_n + X^{r^{n-1}}) \in F[z_2, \dots, z_n][X].$$

The given polynomial relation between the u_i tells us that $g(u_1) = 0$. Consider a monomial $m = cX_1^{b_1} \dots X_n^{b_n}$ appearing in f ($c \in F$). There is a corresponding term

$$cX^{b_1 + rb_2 + \dots + r^{n-1}b_n}$$

appearing in $g(X)$, with all other terms of $g(u_1)$ arising out of m involve the z_i 's and are of lower degree in X . Now choose r sufficiently large to ensure that all the sums

$$b_1 + rb_2 + \dots + r^{n-1}b_n$$

are distinct for all the (finitely many) monomials appearing in f . This ensures that only one monomial in $f(X_1, \dots, X_n)$ contributes to the leading coefficient of $g(X)$. Hence, the leading coefficient of $g(X)$ is a non-zero element of the field F . Rescaling, we can ensure that $g(X)$ is monic, hence u_1 is integral over $F[z_2, \dots, z_n]$. \square

Now focus for a moment on the polynomial algebra $F[X_1, \dots, X_n]$ for F a field. In case $n = 1$, it is a PID so we know the prime ideals are (0) and the (maximal) (f) for $f \in F[X]$ irreducible. But classifying irreducibles is a usually hopeless unless F is *algebraically closed*, in which case the maximal ideals are exactly the $(X - \lambda)$ for $\lambda \in F$. So: *maximal ideals of $F[X]$ for F algebraically closed are parametrized by F .* What can we say if there is more than one variable?

Well, if F be any field, consider $F[X_1, \dots, X_n]$. Given a point $\alpha = (a_1, \dots, a_n) \in F^n$, we have "evaluation at α "

$$e_\alpha : F[X_1, \dots, X_n] \rightarrow F, \quad f(X_1, \dots, X_n) \mapsto f(a_1, \dots, a_n),$$

which is an F -algebra epimorphism. Its kernel is the maximal ideal

$$\ker e_\alpha = (X_1 - a_1, \dots, X_n - a_n)$$

of $F[X_1, \dots, X_n]$. We thus obtain a map

$$F^n \rightarrow \{\text{maximal ideals of } F[X_1, \dots, X_n]\}, \quad \alpha \mapsto \ker e_\alpha.$$

Moreover, this map is injective. (Proof: if $(X_i - b_i) \in (X_1 - a_1, \dots, X_n - a_n)$ then we must have $b_i = a_i$ else $(X_1 - a_1, \dots, X_n - a_n)$ contains a unit contradicting properness.) Now an obvious question arises: are *all* maximal ideals of $F[X_1, \dots, X_n]$ of the form $\ker e_\alpha$ for some $\alpha \in F^n$? Answer: yes *providing* F is algebraically closed...

Hilbert's Nullstellensatz (weak form). *Let F be an algebraically closed field. Then, every maximal ideal of $F[X_1, \dots, X_n]$ is of the form $(X_1 - a_1, \dots, X_n - a_n)$ for $a_1, \dots, a_n \in F$.*

Proof. Let M be a maximal ideal of $R = F[X_1, \dots, X_n]$. Then, $K = R/M$ is a field that is finitely generated as an F -algebra. So by Noether's normalization lemma, K is integral over $F[y_1, \dots, y_r]$ for suitable y_i that are algebraically independent over F . By Lemma 8.4.4, $F[y_1, \dots, y_r]$ is a field, hence $r = 0$. So, K is integral over F , i.e. an algebraic field extension. Finally, since F is algebraically closed, we get that $K = F$. Now let a_i be the image of X_i under the natural homomorphism $R \rightarrow K = F$. Then, M contains $(X_1 - a_1, \dots, X_n - a_n)$. The right hand side is a maximal ideal of R , so we get that $M = (X_1 - a_1, \dots, X_n - a_n)$ as required. \square

Thus, the map

$$F^n \rightarrow \{\text{maximal ideals of } F[X_1, \dots, X_n]\}, \quad \alpha \mapsto \ker e_\alpha$$

is a *bijection* in case F is algebraically closed. So we have determined precisely the maximal ideals of the polynomial ring $F[X_1, \dots, X_n]$ for F an algebraically closed field – they are parametrized by the points in F^n .

This leads us to a very classical setup. View elements $f \in F[X_1, \dots, X_n]$ as functions on the set F^n , so $f(\alpha) = e_\alpha(f) = f(a_1, \dots, a_n)$ for $\alpha = (a_1, \dots, a_n) \in F^n$. Let us call a subset S of F^n an *algebraic set* if S is the set of common zeros of finitely many polynomials in $F[X_1, \dots, X_n]$. Equivalently, since all ideals of $F[X_1, \dots, X_n]$ are finitely generated by Hilbert's basis theorem, a subset S of F^n is algebraic if it is the set of common zeros of an *ideal* I of $F[X_1, \dots, X_n]$.

For example, in two dimensions, the curve $Y = X^2$ in F^2 is an algebraic set, since it is the set of all zeros of the polynomial $Y - X^2 \in F[X, Y]$. Or the union of the X - and Y - axes in F^2 is an algebraic set, as the set of all zeros of the polynomial $XY \in F[X, Y]$. Or the origin in F^2 is an algebraic set, the set of zeros of the polynomials X and Y in $F[X, Y]$. Clearly, understanding algebraic sets is a very classical question to ask!

To make the problem a little more precise, define a map

$$V : \{\text{ideals of } F[X_1, \dots, X_n]\} \rightarrow \{\text{algebraic subsets of } F^n\}$$

by setting

$$V(I) = \{\alpha = (a_1, \dots, a_n) \in F^n \mid f(\alpha) = 0 \text{ for all } f \in I\}.$$

So $V(I)$ is the algebraic subset of F^n defined by the ideal I . (The similarity with the notation $V(I)$ introduced in section 8.3 will be explained shortly!) On the other hand, given an algebraic subset $S \subseteq F^n$, we can associate to it an ideal

$$I(S) = \{f \in F[X_1, \dots, X_n] \mid f(\alpha) = 0 \text{ for all } \alpha \in S\}.$$

Thus we also have a map

$$I : \{\text{algebraic subsets of } F^n\} \rightarrow \{\text{ideals of } F[X_1, \dots, X_n]\}.$$

The maps V and I are both inclusion reversing, and moreover it is obvious that $I(V(J)) \supseteq J, V(I(A)) \supseteq A$ (compare with the maps in the Galois correspondence, section 7.6, equations (1)–(4)). Question: are the maps I and V inverse to one another? At least we have:

8.6.1. Lemma. *If $A \subseteq F^n$ is an algebraic set, $V(I(A)) = A$.*

Proof. If A is an algebraic set, then $A = V(J)$ for some ideal J of $F[X_1, \dots, X_n]$. We know that $I(V(J)) \supseteq J$, and the map V is inclusion reversing, so we get that $V(I(V(J))) \subseteq V(J)$, i.e. $V(I(A)) \subseteq A$. Also, we know that $V(I(A)) \supseteq A$. Hence, $V(I(A)) = A$. \square

So now of course you hope that $I(V(J)) = J$ for all ideals J of $F[X_1, \dots, X_n]$, so that the maps V and I are mutually inverse bijections. But this is *not quite true*:

Hilbert's Nullstellensatz (strong form). If $J \subseteq F[X_1, \dots, X_n]$ is an ideal, $I(V(J)) = \sqrt{J}$.

Proof. Let J be an ideal of R . Clearly, $\sqrt{J} \subseteq I(V(J))$, for if $f \in \sqrt{J}$, then $f^n \in J$ for some n , so $f^n(\alpha) = 0$ for all $\alpha \in V(J)$. But this implies that $f(\alpha) = 0$ for all $\alpha \in V(J)$, i.e. $f \in I(V(J))$.

Conversely, assume that $f(\alpha) = 0$ for all $\alpha \in V(J)$. We have to show that $f \in \sqrt{J}$. Without loss of generality, we may assume $f \neq 0$. Form the ring $R = F[X_1, \dots, X_n, X]$ adjoining a new indeterminate X . Consider the ideal $K = (J, 1 - Xf)$ of R . If K is a proper ideal of R , it has a zero $(a_1, \dots, a_n, a) \in F^{n+1}$ by the weak Nullstellensatz. Then, all elements of J vanish at a_1, \dots, a_n , i.e. $(a_1, \dots, a_n) \in V(J)$. Hence, f vanishes at (a_1, \dots, a_n) . But then $(1 - Xf)(a_1, \dots, a_n, a) = 1 - af(a_1, \dots, a_n) = 1 \neq 0$, a contradiction. Hence, $K = R$.

Therefore, if $J = (j_1, \dots, j_t)$, we can find $h, h_1, \dots, h_t \in R$ such that

$$1 = \sum_{i=1}^n h_i j_i + h(1 - Xf).$$

Replace X by $1/f$ (working in $F[X_1, \dots, X_n]$ localized at $\{1, f, f^2, \dots\}$) to deduce that

$$1 = \sum_{i=1}^n h'_i j_i$$

where each h'_i is a polynomial in X_1, \dots, X_n and $1/f$. Clearing denominators, we obtain an equation

$$f^r = \sum h''_i j_i$$

for some $h''_i \in F[X_1, \dots, X_n]$. This shows $f^r \in J$ as required. \square

Thus, the strong Nullstellensatz tells us that the maps V and I determine a 1-1 correspondence between the algebraic subsets of F^n and the *radical* ideals J of $F[X_1, \dots, X_n]$ (i.e. the ideals J with $J = \sqrt{J}$).

Now I remind you that $\text{Spec } F[X_1, \dots, X_n]$ denotes the set of all prime ideals of $F[X_1, \dots, X_n]$ with the Zariski topology. Maximal ideals are prime ideals, so our map $\alpha \mapsto \ker e_\alpha$ embeds F^n into $\text{Spec } F[X_1, \dots, X_n]$ (the image being the *closed* points). We can then give F^n the subspace topology induced by the topology on $\text{Spec } F[X_1, \dots, X_n]$.

What are the closed sets? Well, there is one for each ideal J of $F[X_1, \dots, X_n]$, and the corresponding closed set $V(J)$ is by definition the set of all maximal ideals containing J . Thus, taking the pre-image, $V(J)$ is the set of all points $\alpha \in F^n$ such that $\ker e_\alpha \supseteq J$, i.e. the set of all points $\alpha \in F^n$ such that α vanishes on all of J . This was exactly what we called the algebraic subset of F^n defined by the ideal J . So we recover the Zariski topology on F^n , the closed sets being the algebraic sets $V(J)$ as J runs over the ideals of $F[X_1, \dots, X_n]$.

Historically, the Zariski topology on F^n (closed sets = zeros of finitely many polynomials) came first. Then it was generalized to the spectrum of prime ideals. The point here is that the former is really only useful to ring theorists when the Nullstellensatz holds, i.e. for finitely generated algebras over algebraically closed fields, while the latter turns out to be helpful when studying arbitrary commutative rings. The Zariski topologies on both F^n and on $\text{Spec } R$ are really the starting point of algebraic geometry...

Finally, suppose that F is an algebraically closed field and that R is a finitely generated commutative F -algebra that is *reduced*, meaning that R has no non-zero nilpotent elements (slightly weaker than assuming R is an integral domain). We may as well assume that R is a quotient of the polynomial ring $F[X_1, \dots, X_n]$ for some n by an ideal J (cf. Lemma 8.5.1). The assumption that R is reduced means that J is a radical ideal, so $J = \sqrt{J}$.

Now, corresponding to J , we have the algebraic set $S = V(J)$ in F^n . Any function f on F^n defines a function \bar{f} on S by restriction. Moreover, for $f, g \in F[X_1, \dots, X_n]$, we have that $\bar{f} = \bar{g}$ if

and only if $(f - g)$ is zero on all of S , i.e. if $(f - g) \in I(S) = I(V(J)) = J$ since $J = \sqrt{J}$. In other words, $\bar{f} = \bar{g}$ if and only if the canonical images of f and g in $R = F[X_1, \dots, X_n]/J$ are equal. So we can view R as a ring of functions on the algebraic set S .

Consider the algebraic subsets of $S = V(J) \subseteq F^n$. By the strong Nullstellensatz, these are in 1–1 correspondence with the radical ideals of $F[X_1, \dots, X_n]$ which contain J . In other words, by the lattice isomorphism theorem, they are in 1–1 correspondence with the radical ideals of R . We have shown:

8.6.2. *The algebraic subsets of $S = V(J)$ are the sets $V(I) = \{\alpha \in S \mid f(\alpha) = 0 \text{ for all } f \in I\}$ as I runs over all ideals of $R = F[X_1, \dots, X_n]/J$. Moreover, given two ideals I, I' of R , $V(I) = V(I')$ if and only if $\sqrt{I} = \sqrt{I'}$.*

You again get (from the weak Nullstellensatz) that the closed sets of S are parametrized by the *maximal* ideals of R , i.e. the closed points in $\text{Spec } R$. So we have identified the algebraic set $S = V(J)$ with the subset of $\text{Spec } R$ consisting of the closed points (the maximal ideals of R).

There is a difference between the two points of view: focusing on the points of $S = V(J)$ depends on the given set of generators of R since we needed to know precisely how R is a quotient of $F[X_1, \dots, X_n]$. But thinking instead of the maximal ideals of R , i.e. the closed points of $\text{Spec } R$, is independent of this choice. If you like, the classical point of view is “basis dependent” while thinking in terms of maximal ideals of $\text{Spec } R$ is choice-independent. Well, we should stop here...