Chapter 2

Affine Varieties

Let R be a ring; which properties of R can be transferred to the polynomial ring $R[X]$? Quite a lot, as we well see. The most important example of such a transfer will be the theorem that if R is a UFD, then so is $R[X]$.

2.1 Polynomial Rings

Let us start with a simple obervation:

Lemma 2.1.1. *R is a domain if and only if $R[X]$ is a domain.*

Proof. We will prove the equivalent statement that R has zero divisors if and only if $R[X]$ has zero divisors.

If R has zero divisors, then clearly so does $R[X]$.

Conversely assume that $f = a_n X^n + \ldots + a_0$ and $g = b_m X^m + \ldots + b_0$ in $R[X]$, where $a_n, b_m \in R \setminus \{0\}$. Then $fg = a_n b_m X^{n+m} + \ldots$, Thus $fg = 0$ implies $a_n b_m = 0$, and R has zero divisors. $\square$

Before we state the next result, let us recall an important characterization of prime elements.

Proposition 2.1.2. *Let R be a domain. Then $p \in R$ is prime if and only if $R/(p)$ is a domain.*

Proof. Assume that p is prime. Recall that $R/(p)$ consists of elements $r + (p)$ (also written $r \bmod p$). We have to show that $R/(p)$ is a domain, so assume that $ab + (p) = 0$. This means $ab \in (p)$, that is, $p \mid ab$. Since p is prime, we have $p \mid a$ or $p \mid p$, which in turn implies $a \in (p)$ or $b \in (p)$. Thus $a + (p) = 0$ or $b + (p) = 0$.

Now let $R/(p)$ be a domain and assume that $p \mid ab$. Then $0 = ab + (p) = (a + (p)) \cdot (b + (p))$, and since $R/(p)$ has no zero divisors, we conclude that $a + (p) = 0$ or $b + (p) = 0$, which implies $p \mid a$ or $p \mid b$. $\square$

Now we show that primes in R remain prime in $R[X]$:

Proposition 2.1.3. *Let R be a domain. If $p \in R$ is prime in R, then it is also prime in $R[X]$.*

Proof. Consider the natural ring homomorphism $\pi : R \longrightarrow R/(p)$. This can be extended to a ring homomorphism $\phi : R[X] \longrightarrow (R/p)[X]$ which sends a polynomial $f = \sum a_i X^i$ to $\overline{f} = \sum \overline{a}_i X^i$, where $\overline{a} = a + (p)$ denotes the residue class of a mod p. The kernel of ϕ consists of all polynomials that are multiples of p, that is, $\ker \phi = pR[X]$. The homomorphism theorem shows that $R[X]/pR[X] \simeq (R/p)[X]$.

Now we find

$$\begin{aligned} p \text{ is prime in R} &\iff R/p \text{ is a domain} \\ &\iff (R/p)[X] \text{ is a domain} \\ &\iff R[X]/pR[X] \text{ is a domain} \\ &\iff p \text{ is prime in R[X].} \end{aligned}$$

Here we have used Lemma 2.1.1, as well as the isomorphism above. □

We can also easily determine the unit group of $R[X]$:

Lemma 2.1.4. *Let R be a domain. Then $R[X]^\times = R^\times$.*

Proof. Clearly any unit in R is also a unit in $R[X]$. Assume therefore that $f = a_m X^m + \ldots + a_0 \in R[X]$ is a unit (in such a situation we will always assume that $a_m \neq 0$). Then there is some $g = b_n X^n + \ldots + b_0 \in R[X]$ such that $fg = 1$. But $fg = a_m b_n X^{m+n} + \ldots$, and since R is a domain, we have $a_m b_n \neq 0$. But then we must have $m + n = 0$, hence $m = n = 0$, and this shows that $f, g \in R$. □

Unique Factorization

Now we are ready to give the main result of this section:

Theorem 2.1.5. *If R is a UFD, then so is $R[X]$.*

Since $\mathbb{Z}$ and any field K are unique factorization domains, so are $\mathbb{Z}[X]$ and $K[X]$. Applying the theorem again shows that $\mathbb{Z}[X, Y]$ and $K[X, Y]$ are UFDs. By induction, the same holds for the polynomial rings $\mathbb{Z}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$.

The proof of Theorem will first be reduced to the case of 2primitive" polynomials. For any $f \in R[X]$, let a be the gcd of the coefficients of f. Then $f = ag$, where $g \in R[X]$ is a polynomial whose coefficients have gcd equal to 1 (such polynomials are called primitive).

Now let $f \in R[X]$, and write $f = ag$ for g primitive. If we can show that g has a factorization into irreducibles, then the same must be true for f because we know that constants have such a factorization. Similarly, if we can show that primitive polynomials have unique factorization, then this is true for general polynomials. For assume that $f = ag$ with $a \in R$ and g primitive,

and assume that $f = bh$ is a second factorization into polynomials b, h. Since $a = p_1 \cdots p_r$ has a factorization into primes, each p_i divides bh and therefore b or h. Cancellation yields $g = b_1 h_1$, and since g has unique factorization, the same is true for $f = ag = p_1 \cdots p_r \cdot g$ (we just proved that every irreducible factor of a also occurs as a factor (up to a unit) in the second factorization $f = bh$).

Let us first prove the existence of a factorization:

Lemma 2.1.6. *Let R be a UFD. Then every $f \in R[X]$ can be written as a product of a unit and of irreducible elements.*

Proof. We do induction on $\deg f$. We have seen that we may assume that f is primitive. Thus if $\deg f = 0$, then f must be a unit, and we are done.

Now assume that every polynomial with degree $< n$ has a factorization into irreducible elements, and assume that $\deg f = n$. If f is irreducible, then we are done. If not, then $f = gh$ with $\deg g, \deg h < n$ (here we use that f is primitive, i.e., not divisible by irreducible constants). Then g and h can be factored into irreducibles by induction assumption, hence the same is true for $f = gh$. $\square$

For proving uniqueness we will also use induction on the degree of f. If $\deg f = 0$, then $f \in R$. Any factorization of f into irreducibles involves only elements in R, and since factorization in R is unique, f has at most one factorization (up to shuffling the factors or units, as usual).

Now assume that every polynomial with degree $< n$ is unique. Assume moreover that f has degree $n > 0$ and two different factorizations into irreducible elements into irreducible factors of degree > 0. Let p be a factor of minimal degree and write $f = pg$. Let q be a factor of minimal degree in the second factorization, and write $f = qh$. If p divides q or h, cancelling p again shows that both factorizations are essentially the same. Thus we may assume that $p \nmid q$ and $p \nmid h$.

Since $\deg p \leq \deg q$ we can write $p = ax^m + \ldots$ and $q = bx^n + \ldots$ with $m \leq n$. Now consider the polynomial $F = (bx^{n-m}p - aq)h$. If $F = 0$, then clearly $p \mid aq$. If $F \neq 0$, then $\deg F < \deg qh = n$, so F has unique factorization by induction assumption. Now observe

$$F = (bx^{n-m}p - aq)h = p(bx^{n-m} - ak).$$

Since F has unique factorization, the irreducible factor p also occurs in the first factorization. Since $p \nmid h$, we conclude that $p \mid (bx^{n-m}p - aq)$ and therefore $p \mid aq$.

Thus we have $p \mid aq$ in both cases. Since $\deg aq = \deg q < n$, aq has unique factorization. From $\deg a = 0$ we conclude that p must be a factor of q, but this contradicts $p \nmid q$, and we are done.

Note that $R[X]$ is in general not a principal ideal domain even if R is: for example, $R = \mathbb{Z}$ is a PID, but the ideal $(2, X)$ in $\mathbb{Z}[X]$ is not principal.

2.2 Noetherian Rings

There is one more important property that polynomial rings $R[X]$ inherit from R: that of being noetherian.

A noetherian ring is a (commutative) ring with 1 in which every ascending chain of ideals terminates. In other words: if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ is an ascending chain of ideals, then there is some index n such that $I_n = I_{n+1} = \ldots$.

Proposition 2.2.1. *A ring R is Noetherian if and only if every ideal in R is finitely generated.*

Proof. Assume that R is Noetherian and let I be an ideal in R. If $I = (0)$, we are done; if not, pick an element $a_1 \in I \setminus (0)$. If $I = (a_1)$, we are done; if not, pick an element $a_2 \in I \setminus (a_1)$. If $I = (a_1, a_2)$, we are done; if not, pick $a_3 \in I \setminus (a_1, a_2)$ and continue. In this way we get an ascending chain of ideals

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \ldots.$$

Since R is Noetherian, this process must terminate, say at $(a_1, \ldots, a_n)$, and then I is generated by $a_1, \ldots, a_n$.

Now assume that every ideal in R is finitely generated. Assume we have an ascending chain

$$I_1 \subsetneq I_2 \subsetneq \ldots$$

of ideals. Let I be the union of these I_j; then I is an ideal, hence finitely generated, say $I = (a_1, \ldots, a_n)$. Each of these elements lies in some I_j; let m be the maximal index occurring. Then $I \subseteq I_m$, hence $I_m = I_{m+1} = \ldots$. $\square$

As an immediate corollary we have

Corollary 2.2.2. *Principal ideal domains are Noetherian.*

Also note that ideals in rings of integers in an algebraic number field always can be generated by at most two algebraic integers; in particular, these rings are Noetherian.

As an example of a ring that is not Noetherian, consider the polynomial ring $R = \mathbb{Q}[X_1, X_2, X_3, \ldots]$ of infinitely many variables. The ideal $(X_1, X_2, \ldots)$ in R is not finitely generated; alternatively, the sequence

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \ldots$$

is an ascending chain of ideals that does not terminate. Note that the quotient field $K = \mathbb{Q}(X_1, X_2, X_3, \ldots)$ is Noetherian (any field is); since R is a subring of K, this shows that not every subring of a Noetherian ring is Noetherian. Actually, even the 'sandwich argument' does not work for Noetherian rings: we have $\mathbb{Q} \subset R \subset K$ with $\mathbb{Q}$ and K Noetherian, and yet R is not.

The following obervation is simple but useful:

Proposition 2.2.3. *Let I be an ideal in some Noetherian ring R. Then R/I is Noetherian.*

Proof. Let J be an ideal in R/I, and consider the ideal J_0 in R defined by $J_0 = \{r : r + (I) \in J\}$. Then J_0 is an ideal, hence generated by $x_1, \ldots, x_n \in R$. But then R/I is generated by $x_1 + I, \ldots, x_n + I$. $\square$

A big source of Noetherian rings are polynomial rings $K[X_1, \ldots, X_n]$:

Theorem 2.2.4 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then so is $R[X]$.*

Proof. Let I be an ideal in $R[X]$. We claim that I is finitely generated. Choose $f_1 \in I \setminus (0)$ with minimal degree; if $I \neq (f_1)$, choose $f_2 \in I \setminus (f_1)$ with minimal degree. If this process terminates, we are done. If not, let a_i be the leading coefficient of f_i, and form the ideal $J = (a_1, a_2, a_3, \ldots)$ in R. Since R is Noetherian, we have $J = (a_1, \ldots, a_N)$ for some N.

We now claim that $I = I_N := (f_1, \ldots, f_N)$. If not, then $f_{N+1} \in I \setminus I_N$. Moreover, $a_{N+1} = \sum_{i=1}^{N} r_i a_i$ since $a_{N+1} \in J$. Now set

$$g = \sum_{i=0}^{N} r_i f_i x^{\deg f_{N+1} - \deg f_i}.$$

Since g is a linear combination of the f_i, we have $g \in I_N$. Next $\deg g = \deg f_{N+1}$, and both polynomials have the same leading term. Thus $\deg(f_{N+1} - g) < \deg f_{N+1}$, hence $f_{N+1} - g \in I \setminus I_N$; but this contradicts the minimality of $\deg f_{N+1}$. $\square$

2.3 Affine Varieties

We now will start setting up a dictionary between the algebraic side (the polynomial ring $R = K[X_1, \ldots, X_n]$ and ideals in this ring) and the geometric side (zero sets of systems of polynomials in R). Eventually this will allow us to transfer terms like tangent spaces, singular points, parametrizations etc. to the algebraic side; the idea still is to use your geometric intuition for solving a problem algebraically.

From Ideals to Varieties

Let K be a field and $R = K[X_1, \ldots, X_n]$. We also define the affine n-space to be $\mathbb{A}^n K = \{(x_1, \ldots, x_n) : x_i \in k\}$. For every set $S \subseteq R$ we define the vanishing set $\mathcal{V}(S)$ as

$$\mathcal{V}(S) = \{P \in \mathbb{A}^n K : f(P) = 0 \text{ for all } f \in S\}.$$

For example, $\mathcal{V}(R) = \varnothing$ and $\mathcal{V}(\{0\}) = \mathbb{A}^n K$.

If S, S' are subsets of R with $S \subseteq S'$, then clearly $\mathcal{V}(S') \subseteq \mathcal{V}(S)$. Let I be the ideal in R generated by S. Then I claim that $\mathcal{V}(S) = \mathcal{V}(I)$. Since $S \subseteq I$, we only have to show that $\mathcal{V}(S) \subseteq \mathcal{V}(I)$. Thus let $P \in \mathbb{A}^n K$ be a point with $f(P) = 0$ for all $f \in S$. Then we have to show that $g(P) = 0$ for all $g \in I$. But every such g can be written in the form $g = \sum r_i f_i$ for $r_i \in R$ and $f_i \in S$, hence $g(P) = \sum r_i f_i(P) = 0$.

Thus when talking about vanishing sets $\mathcal{V}(I)$ we may always assume that I is an ideal in R. Since R is Noetherian, I will be finitely generated, and this means we always have $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_n)$: every vanishing set is the vanishing set of a finite number of polynomials because of Hilbert's Basis Theorem.

Vanishing sets are also called algebraic sets. The map

$$\mathcal{V} : \{\text{ideals in } R\} \longrightarrow \{\text{algebraic sets in } \mathbb{A}^n K\}$$

sending an ideal I to $\mathcal{V}(I)$ is, as we have already seen, inclusion reversing ($I \subseteq J$ implies $\mathcal{V}(I) \supseteq \mathcal{V}(J)$; this is even true for sets). In addition, it has the following basic properties:

Lemma 2.3.1. *1. $\mathcal{V}(0) = \mathbb{A}^n K$; $\mathcal{V}(R) = \varnothing$;*

2. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$;

3. $\mathcal{V}(\sum I_\nu) = \bigcap \mathcal{V}(I_\nu)$.

Here I, J, I_ν are ideals in R, and $\sum I_\nu$ denotes the ideal consisting of finite R-linear combinations of elements in the I_ν.

Proof. 1. These properties are clear.

2. We have $\mathcal{V}(I) \subset \mathcal{V}(I \cap J)$ since $I \cap J \subset I$. Similarly $\mathcal{V}(J) \subset \mathcal{V}(I \cap J)$, hence $\mathcal{V}(I) \cup \mathcal{V}(J) \subset \mathcal{V}(I \cap J)$.

Now assume that $P \in \mathcal{V}(I \cap J)$. If P is not in $\mathcal{V}(I)$, then there is some $f \in I$ with $f(P) \neq 0$. Similarly, if P is not in $\mathcal{V}(J)$, then there is some $g \in J$ with $g(P) \neq 0$. Then $fg \in I \cap J$ and $fg(P) \neq 0$: contradiction.

3. Let $P \in \bigcap \mathcal{V}(I_\nu)$; then $f_\nu(P) = 0$ for all $f_\nu \in I_\nu$, hence $f(P) = 0$ for all finite linear combinations $f \in \sum I_\nu$. This shows that $\bigcap \mathcal{V}(I_\nu) \subseteq \mathcal{V}(\sum I_\nu)$.

On the other hand, $I_\mu \subset \sum I_\nu$ for every μ, hence $\mathcal{V}(\sum I_\nu) \subseteq \mathcal{V}(I_\mu)$ for every μ, and therefore $\mathcal{V}(\sum I_\nu) \subseteq \bigcap \mathcal{V}(I_\mu)$. $\square$

Now recall the definition of a topological space: it is a set X, together with a family $\mathcal{O}$ of subsets (called open sets) with the following properties:

- $\varnothing \in \mathcal{O}$, $X \in \mathcal{O}$;
- $U, V \in \mathcal{O}$ implies $U \cap V \in \mathcal{O}$;
- $U_i \in \mathcal{O}$ implies $\bigcup U_i \in \mathcal{O}$.

In this topological space $(X, \mathcal{O})$, we say that a subset $A \subset X$ is closed if $X \setminus A$ is open. This means that the family $\mathcal{C}$ of closed sets has the following properties:

- $\varnothing \in \mathcal{O}$, $X \in \mathcal{O}$;
- $U, V \in \mathcal{O}$ implies $U \cup V \in \mathcal{O}$;
- $U_i \in \mathcal{O}$ implies $\bigcap U_i \in \mathcal{O}$.

Equivalently, we may define a topology by saying what its closed sets are and defining open sets as the complements of closed sets.

Comparing Lemma 2.3.1 with the definition above we see that algebraic sets in $\mathbb{A}^n K$ form the closed sets of a topology on $\mathbb{A}^n K$; this topology is called the Zariski topology.

Lemma 2.3.2. *The Zariski-closed sets in $\mathbb{A}^1 K$ are the finite subsets (finite sets of points) and $\mathbb{A}^1 K$ itself.*

From Varieties to Ideals

Assume that V is an affine algebraic set, defined as the zero set of polynomials $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. For any $P = (a_1, \ldots, a_n) \in V$ we have $f_j(P) = 0$. Thus $f(P) = 0$ for any K-linear combination f of the f_i. This shows that $f(a) = 0$ for all $f \in (f_1, \ldots, f_n)$. Thus we are led to define the vanishing ideal

$$\mathcal{I}(V) = \{f \in K[X_1, \ldots, X_n] : f(P) = 0 \text{ for all } P \in V\}$$

of the algebraic set V. Note that $\mathcal{I}(\varnothing) = K[X_1, \ldots, X_n]$. If K has infinitely many elements, then $\mathcal{I}(\mathbb{A}^n K) = (0)$, but observe that e.g. $\mathcal{I}(\mathbb{A}^1 \mathbb{F}_2) = (X(X - 1)) \neq (0)$.

It is also clear from the definition that $\mathcal{I}$ is inclusion reversing: if $V_1 \subseteq V_2$ are affine algebraic sets, then $\mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$.

Lemma 2.3.3. *For any algebraic set V we have $\mathcal{V}(\mathcal{I}(V)) = V$.*

Proof. We clearly have $V \subseteq \mathcal{V}(\mathcal{I}(V))$: if $f \in \mathcal{I}(V)$, then $f(P) = 0$ for any $P \in V$, hence $P \in \mathcal{V}(\mathcal{I}(V))$.

Now assume that V is the zero set of polynomials $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. Then $f_1, \ldots, f_m \in \mathcal{I}(V)$, hence $(f_1, \ldots, f_m) \subseteq \mathcal{I}(V)$, and therefore $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(f_1, \ldots, f_m) = V$. □

The map $\mathcal{I}$ seems to have similar properties:

Lemma 2.3.4. *For any ideal I in R we have $I \subseteq \mathcal{I}(\mathcal{V}(I))$.*

Proof. Let $f \in I$. Then $f(P) = 0$ for any $P \in \mathcal{V}(I)$, and this shows that $f \in \mathcal{I}(\mathcal{V}(I))$. □

If we could prove the converse inclusion, then every ideal I would have the form $I = \mathcal{I}(V)$ for some algebraic set V. Unfortunately, this is not true: the ideal $I = (X^2)$ in $K[X, Y]$, for example, is not of the form $\mathcal{I}(V)$: in fact, assume that $\mathcal{I}(V) = I$. Then $V = \mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(I)$, hence V consists of the y-axis. But then $\mathcal{I}(V) = (X)$, and this ideal is strictly larger than I.

There is a second problem: if we work in the affine plane over $K = \mathbb{R}$, then $\mathcal{V}(I) = \varnothing$ for $I = (X^2 + Y^2 + 1)$, whereas $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\varnothing) = \mathbb{R}[X, Y] \neq I$. Thus if we want a bijection between ideals and algebraic sets, then we will have to assume that K is algebraically closed.

In order to clarify the first problem, let us introduce the radical $\operatorname{rad} I$ of an ideal I in any ring R by

$$\operatorname{rad} I = \{f \in R : f^m \in I \text{ for some } m \in \mathbb{N}\}.$$

It is an easy exercise to check that $\operatorname{rad} I$ is an ideal; the only difficulty consists in showing that $\operatorname{rad} I$ is closed under addition: assume that $f, g \in \operatorname{rad} I$. Then $f^n, g^m \in I$ for suitably chosen integers $n, m \geq 0$, hence $(f+g)^r = \sum \binom{r}{k} f^k g^{r-k} \in I$ as soon as $r \geq m+n-1$.

Note that $I \subseteq \operatorname{rad} I$ for every ideal I. Moreover, $\operatorname{rad}(X^2) = (X)$. Finally observe that if R is a UFD and $f = f_1^{a_1} \cdots f_n^{a_n}$, then $\operatorname{rad}(f) = (f_1 \cdots f_n)$. Compare this with our use of rad in Mason's theorem.

Proposition 2.3.5. *If V is an algebraic set, then $\mathcal{I}(V) = \operatorname{rad} \mathcal{I}(V)$.*

Thus vanishing ideals have the property that they coincide with their radical. In particular, (X^2) can never be the vanishing ideal of an algebraic set because $\operatorname{rad}(X^2) = (X)$.

Proof. Since $I \subseteq \operatorname{rad} I$ for any ideal I, we only have to show that $\operatorname{rad} \mathcal{I}(V) \subseteq \mathcal{I}(V)$. Assume therefore that $f \in \operatorname{rad} \mathcal{I}(V)$. Then $f^n \in \mathcal{I}(V)$ for some n, hence $f^n(P) = 0$ for all $P \in V$. But this implies $f(P) = 0$, hence $f \in \mathcal{I}(V)$. $\square$

Thus we only can hope to get a bijection between affine algebraic sets and radical ideals (these are ideals that coincide with their radical). This is exactly what happens:

Proposition 2.3.6. *For any ideal I in R we have $\mathcal{I}(\mathcal{V}(I)) = \operatorname{rad} I$.*

One direction is easy to prove: we have $\operatorname{rad} I \subseteq \mathcal{I}(\mathcal{V}(I))$. In fact, let $f \in \operatorname{rad} I$. Then $f^m \in I \subseteq \mathcal{I}(\mathcal{V}(I))$ (here we used Lemma 2.3.4). By definition of the radical this means $f \in \operatorname{rad} \mathcal{I}(\mathcal{V}(I))$. Now apply Prop. 2.3.5.

The proof of the converse inclusion is highly nontrivial; actually it is a consequence of Hilbert's Nullstellensatz, which we will prove below.

2.4 Hilbert's Nullstellensatz

We now recall the definition of prime and maximal ideals (we have already discussed prime elements at the beginning of this chapter). An ideal $\mathfrak{p}$ in a ring is prime if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$; it is then easily seen that $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain. In fact, assume that $R/\mathfrak{p}$ is a domain, and let $ab \in \mathfrak{p}$. Then $0 = ab + \mathfrak{p} = (a+\mathfrak{p})(b+\mathfrak{p})$, and since $R/\mathfrak{p}$ is a domain, we get $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$: thus $\mathfrak{p}$ is prime. Conversely, if $\mathfrak{p}$ is prime and $(a+\mathfrak{p})(b+\mathfrak{p}) = 0$, then $ab \in \mathfrak{p}$, hence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, and this shows that $R/\mathfrak{p}$ is a domain.

Moreover, an ideal $\mathfrak{m}$ is maximal if $\mathfrak{m} \subseteq \mathfrak{n} \subseteq R$ for some ideal $\mathfrak{n}$ implies that $\mathfrak{m} = \mathfrak{n}$ or $\mathfrak{n} = R$; again it is easy to see that $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.

Since fields are domains, maximal ideals are always prime; the converse, however, is not true in general. Consider e.g. the domain $R = K[X, Y, Z]$; here $(X) \subset (X, Y) \subset (X, Y, Z)$ is an ascending chain of prime ideals, but only the last one is maximal. This can be seen most easily from the isomorphisms $K[X, Y, Z]/(X) \simeq K[Y, Z]$ (a domain, but not a field), $K[X, Y, Z]/(X, Y) \simeq K[Z]$ (also a domain, but not a field) and $K[X, Y, Z]/(X, Y, Z) \simeq K$ (a field).

Let us discuss the first isomorphism in detail: it is induced by the ring homomorphism $\phi : K[X, Y, Z] \longrightarrow K[Y, Z]$ defined by $f(X, Y, Z) \longmapsto f(0, Y, Z)$, which is clearly surjective and whose kernel consists of (X): clearly, any multiply of X is in the kernel, so we have to prove the inverse. Assume therefore that $f \in \ker \phi$; this means $f(0, Y, Z) = 0$. Now in polynomial rings $F[X]$ in one variable over a field F we know that $g(X) = 0$ if and only if $g(X) = Xh(X)$, i.e. $g \in (X)$. The problem is that $K[X, Y, Z]$ is not a polynomial ring in one variable over a field. Here's what we do: clearly $K[X, Y, Z] \subseteq F[X]$, where $F = K(X, Y)$ is a field. in $F[X]$ we can write $g(X) = X \cdot h(X)$, where h is a polynomial in X whose coefficients are polynomials in Y and Z. Multiply through by the lowest common multiple $G(Y, Z)$ of the denominators; then $g(X, Y, Z)G(Y, Z) = XH(X, Y, Z)$ for $G, H \in R$. Now X is prime in R, hence divides g or G. But it cannot divide G unless $G = 0$ (if $X \mid G$, say $G = XG_1$, plug in $X = 0$, and you get $G(Y, Z) = 0$). Since $G \neq 0$, we must have $X \mid g$ as claimed. There probably is a much simpler proof that I will put here as soon as my head clears up.

OK, here comes: f is a sum of monomials $a_{ijk}X^iY^jZ^k$. Collect those divisible by X and write $f(X, Y, Z) = XF(X, Y, Z) + G(Y, Z)$: here G is the sum of those terms not divisible by X. Now plug in $X = 0$. You will find $f(0, Y, Z) = G(Y, Z)$. Thus $f \in \ker \phi$ if and only if $G = 0$, which means f is a multiple of X.

Study the details of this argument until you are sure that you can do similar things without a problem.

Remark. Ascending chains of prime ideals can be used to define the dimension of rings: the Krull dimension of a ring R is the length of the maximal ascending chain of prime ideals in R. The chain $(X) \subset (X, Y) \subset (X, Y, Z)$ shows that $\text{K-dim}\, K[X, Y, Z] \geq 3$, and it can be shown that we have equality here.

For the rest of this chapter, let K be an algebraically closed field.

Theorem 2.4.1 (Weak Nullstellensatz)**.** *Let K be an algebraically closed field. Then every maximal ideal in the polynomial ring $R = K[X_1, \ldots, X_n]$ has the form $M = (X_1 - a_1, \ldots, X_n - a_n)$ for some point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n K$.*

Note that the weak Nullstellensatz gives us a bijection between maximal ideals in $K[X_1, \ldots, X_n]$ and points in $\mathbb{A}^n K$. Also observe that the theorem does not hold for arbitrary fields: in $\mathbb{R}[X]$, the ideal $M = (X^2 + 1)$ is maximal because $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ is a field, yet M is not of the form $(X - a)$ for some $a \in \mathbb{R}$.

As a consequence we have

Corollary 2.4.2 (Nullstellensatz)**.** *Let K be an algebraically closed field and $I \neq (1)$ be an ideal in $K[X_1, \ldots, X_n]$. Then $\mathcal{V}(I) \neq \varnothing$.*

This is definitely a good thing to know: the corollary states that, over algebraically closed field, every algebraic set $\mathcal{V}(I)$ with $I \neq R$ actually has a point, in other words: the polynomials f_i generating I have a common zero.

Proof. If $I \neq R = K[X_1, \ldots, X_n]$, then there is some maximal ideal M with $I \subseteq M$ (this follows from the ascending chain condition: if I is maximal, we are done; if not then there is some I_1 sandwiched between I and R; now repeat and observe that this process must end eventually). Now $M = (X_1 - a_1, \ldots, X_n - a_n)$ by the weak Nullstellensatz, hence $f(P) = 0$ for $P = (a_1, \ldots, a_n)$ and any $f \in I$. In particular, $P \in \mathcal{V}(I)$. $\square$

Another consequence is

Corollary 2.4.3. *For any ideal I in $R = K[X_1, \ldots, X_n]$ we have $\mathcal{I}(\mathcal{V}(I)) = \operatorname{rad} I$. In particular, if I is a radical ideal, then $\mathcal{I}(\mathcal{V}(I)) = I$.*

Thus $\mathcal{I}$ and $\mathcal{V}$ set up a one-to-one correspondence between radical ideals in $K[X_1, \ldots, X_n]$ and affine algebraic sets in $\mathbb{A}^n K$.

Proof. We already know $\operatorname{rad} I \subseteq \mathcal{I}(\mathcal{V}(I))$. For proving the converse relation, write $I = (f_1, \ldots, f_m)$ and take some $g \in \mathcal{I}(\mathcal{V}(I))$. We know that $g(P) = 0$ for any $P \in \mathcal{V}(I)$. We have to prove that $g \in \operatorname{rad} I$, or, equivalently, that some power of g lies in I.

The following proof is called the trick of Rabinowitsch. Adjoin a new variable X_{n+1} to R, i.e., let $S = R[X_{n+1}]$. Then the polynomials $f_1, \ldots, f_m$ and $X_{n+1}g - 1$ have no common zeros in $\mathbb{A}^{n+1}K$: In fact, the common zeros of the f_i are the points $Q = (x_1, \ldots, x_n, x_{n+1})$ with $P = (x_1, \ldots, x_n) \in V = \mathcal{V}(I)$. Is any of these points Q also a zero of $X_{n+1}g - 1$? Plugging in Q gives $x_{n+1}g(P) - 1 = -1$, since $g \in \mathcal{I}(V)$ implies $g(P) = 0$.

Thus $\mathcal{V}(f_1, \ldots, f_m, X_{n+1}g - 1) = \varnothing$. By the weak Nullstellensatz we must have $(f_1, \ldots, f_m, X_{n+1}g - 1) = (1) = S$, and this implies that 1 is a linear combination of the generators:

$$1 = p_1 f_1 + \ldots + p_m f_m + p_{m+1}(X_{n+1}g - 1),$$

where $p_j \in S$. Now plug in $X_{n+1} = \frac{1}{g}$ (the result will be an element in $K(X_1, \ldots, X_n)$. This gives

$$1 = p_1(x_1, \ldots, x_n, 1/g) f_1 + \ldots + p_m(x_1, \ldots, x_n, 1/g) f_m.$$

Now multiply through by a power of g to clear denominators; the resulting equation then shows that this power of g is in I. $\square$

For the proof of the Nullstellensatz we need the following lemma (whose proof is due to D. Allcock):

Lemma 2.4.4. *Let k be a field and K/k an extension which is finitely generated as a k-algebra. Then K/k is algebraic.*

We will give the proof later; for now let me explain what this means. Recall that an algebra is, cum grano salis, a vector space in which vectors can be multiplied. For example, the polynomial ring $A = K[X_1, \ldots, X_n]$ is also a K-vector space and therefore a K-algebra: elements in A can be added (as vectors), multiplied by scalars from K, and can be multiplied as polynomials.

If K/k is a field extension, then we can interpret K as a k-vector space: we can add and subtract elements of K and multiply them by the "scalars" from k. Since the "vectors" in K can also be multiplied as elements of K, we see that K actually is a k-algebra.

A k-algebra K is now said to be finitely generated if there are elements α_1, $\ldots$, α_m such that every $\alpha \in K$ can be written as a k-linear combination of products of the α_i; in other words: if the k-algebra generated by the α_i is equal to K.

As an example, consider the $\mathbb{Q}$-algebra $\mathbb{Q}(X)$ of rational functions in one variable X. The $\mathbb{Q}$-algebra generated by $f = \frac{1}{X}$ and $g = \frac{X-1}{X+1}$ consists of all $\mathbb{Q}$-linear combinations of f, g, f^2, fg, g^2, $\ldots$. Note that all such elements have poles at most at $x = 0$ and $x = -1$.

Now we claim that $\mathbb{Q}(X)$ is not finitely generated as a $\mathbb{Q}$-algebra. If it were, then there would be rational functions $f_1, \ldots, f_n$ such that every rational function $f \in \mathbb{Q}(X)$ can be written as a linear combination of products of the f_j. But this is not possible: the f_i have finitely many poles, and by forming products and linear combinations no new poles are created. Thus if $a \in \mathbb{Q}$ is not one of the finitely many poles, then $\frac{1}{X-a}$ is not an element of the $\mathbb{Q}$-algebra generated by the f_i.

Proof of the Weak Nullstellensatz. Let $\mathfrak{m}$ be a maximal ideal in R. Then $R/\mathfrak{m}$ is a field. Moreover, it is obviously finitely generated as a k-algebra, namely by the elements $X_1 + \mathfrak{m}$, $\ldots$, $X_n + \mathfrak{m}$: every element in R is a k-linear combination of products of the X_i, hence every element in $R/\mathfrak{m}$ is a k-linear combination of products of the $X_i + \mathfrak{m}$. Observe that $R/\mathfrak{m}$ contains k as a subfield: the map $\phi : k \longrightarrow R/\mathfrak{m}; a \longmapsto a + \mathfrak{m}$ is a ring homomorphism, and we have $\ker \phi = \{a \in k : a \in \mathfrak{m}\} = k \cap \mathfrak{m}$. If $\mathfrak{m}$ contains a nonzero element $a \in k$, then it contains 1 and is therefore equal to R. Since $\mathfrak{m}$ is maximal, this cannot happen, hence $k \cap \mathfrak{m} = (0)$, and ϕ is injective.

Thus $R/\mathfrak{m}$ is a field extension of k, and by Lemma 2.4.4 we find that it is algebraic over k. But k is algebraically closed, hence $R/\mathfrak{m} = k$.

Now consider the natural projection $\pi : R \longrightarrow R/\mathfrak{m} = k$ sending $f \in R$ to the coset $f + \mathfrak{m}$. Since $\pi(x_j) = a_j$ for $a_j \in k$, the elements $x_j - a_j$ are in the kernel of π, which is by definition just $\mathfrak{m}$. Thus $\mathfrak{m}$ contains $(X_1 - a_1, \ldots, X_n - a_n)$; this last ideal is maximal, and since $\mathfrak{m}$ is also maximal, we must have equality: $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$. $\square$

In order to get an idea for the proof of Lemma 2.4.4, let us first consider the special case where k is infinite and where $K = k(X)$ is a simple transcendental

extension. Our claim is that if $f_1, \ldots, f_m \in K$, then the k-algebra A they generate is strictly smaller than K. In fact, choose $a \in k$ such that a is not a pole of any of the rational functions f_j; then no element of A can have a pole at a, hence $\frac{1}{X-a} \in K \setminus A$.

Now we complete the proof of the Nullstellensatz by proving the central lemma:

Proof of Lemma 2.4.4. In order to simplify the presentation, we will assume that k is algebraically closed, although the proof for general fields k is only slightly more complicated.

We first give the proof for fields K with transcendence degree 1 over k and then do the general case later. Recall that K/k has transcendence degree 1 if there is some $X \in K$ such that $K/k(X)$ is finite.

As before, let $f_1, \ldots, f_m \in K$, and let A be the k-algebra these rational functions generate. Since $K/k(X)$ is finite, there exist elements $e_1, \ldots, e_n \in K$ that form a basis for the vector space K over $k(X)$. The product $e_i e_j$ of two basis elements can be expressed as a $k(X)$-linear combination of the e_h, hence there exist polynomials $a_{ijh}, b_{ijh} \in k[X]$ with

$$e_i e_j = \sum_h \frac{a_{ijh}(X)}{b_{ijh}(X)} e_h.$$

We also can express our f_i in terms of this basis:

$$f_i = \sum_j \frac{c_{ij}(X)}{d_{ij}(X)} e_j$$

for polynomials $c_{ij}, d_{ij} \in k[X]$.

Now observe that the poles of the elements in A must come from the finitely many poles of the e_j, the roots of the finitely many polynomials d_{ij}, or the roots of the finitely many polynomials b_{ijh}. Thus there is some $a \in k$ (here we use that k is algebraically closed) that is not among these poles, and then $\frac{1}{X-a} \in K \setminus A$.

Now let us do the general case of fields K with arbitrary transcendence degree ≥ 1. Let F be a subextension of K such that K/F has transcendence degree 1. From what we have proved we know that K is not a finitely generated F-algebra; this immediately shows that it is not a finitely generated k-algebra. $\square$

Exercises

4.1 Let R be a domain, and $S \neq \varnothing$ a multiplicatively closed subset of R (this means that $ss' \in S$ for $s, s' \in S$) not containing 0. On the set of pairs $(r, s) \in R \times S$ define a relation $(r, s) \sim (r', s')$ if $rs' = r's$.

1. Show that $\sim$ is an equivalence relation.

2. Let $\frac{r}{s}$ denote the equivalence class of (r, s), and put

$$S^{-1}R = \{\tfrac{r}{s} : r \in R, s \in S\}.$$

Define addition and multiplication on $S^{-1}R$ by $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ and $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$. Show that this is well defined and makes $S^{-1}R$ into a domain. Also show that the map $R \longrightarrow S^{-1}R : r \longmapsto \frac{rs}{s}$ for a fixed $s \in S$ is an injective ring homomorphism.

3. Show that $S^{-1}R$ is a field if $S = R \setminus \{0\}$; it is called the quotient field of R.

4.2 Show that $p \in R$ is a unit in $S^{-1}R$ if and only if $p \mid s$ for some $s \in S$.

4.3 Let $p \in R$ be a prime element, and assume that $p \nmid s$ for all $s \in S$. Show that p is prime in $S^{-1}R$.

4.4 Show that if R is a UFD, then so is $S^{-1}R$.

4.5 Show that if R is noetherian, then so is $S^{-1}R$. Hint: If I is an ideal in $S^{-1}R$, consider $J = I \cap R$. Show that generators of J also generate I.

4.6 Show that prime ideals are radical.

4.7 Show that radical ideals are radical: $\operatorname{rad}(\operatorname{rad} I) = \operatorname{rad} I$.

4.8 Show that $K[X, Y, Z]/(X, Y) \simeq K[Z]$ and $K[X, Y, Z]/(X, Y, Z) \simeq K$.

4.9 Show that an integral domain R is a UFD if and only if

- every ascending chain of *principal* ideals terminates, and
- irreducibles are prime.

4.10 Consider the ideal $I = (XY, YZ, ZX)$ in $K[X, Y, Z]$. Describe $\mathcal{V}(I)$ in $\mathbb{A}^3K$. Is $I = \mathcal{I}(\mathcal{V}(I))$?

4.11 Let $I = (X^2 + Y^2 - 1, Y - 1)$; find $f \in \mathcal{I}(\mathcal{V}(I)) \setminus I$.