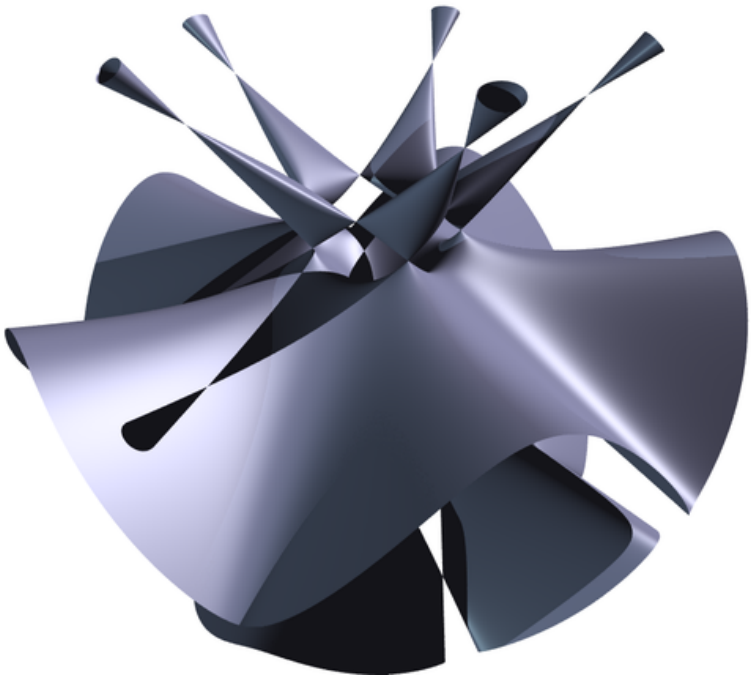
(Topics in) Algebra I

MAT 4141/5141

Fall 2018



Alistair Savage

Department of Mathematics and Statistics

University of Ottawa

Contents

Preface

These are notes for the cross-listed courses *Algebra I* (MAT 5141) and *Topics in Algebra I* (MAT 4141) at the University of Ottawa. This is a second course in rings and modules. We assume that students are familiar with the basic theory of rings (e.g. course MAT 3143 at uOttawa) and modules (e.g. course MAT 3141 at uOttawa).

We begin with the concepts of noetherian and artinian modules. We then turn our attention to some basic commutative algebra, including the concepts of affine varieties, the Hilbert Basis Theorem, Hilbert's Nullstellensatz, localization, and tensor products. We then cover the theory of semisimple modules and rings, including Schur's Lemma, the Jacobson Density Theorem, and the Artin–Wedderburn Theorem. We conclude with a brief introduction to homomological algebra, including short exact sequences and projective, injective, and flat modules.

Acknowledgements: Portions of these notes closely follow the textbook [Ash].

Alistair Savage

Course website: `http://alistairsavage.ca/mat5141`

Chapter 1

Noetherian and artinian modules and rings

In this chapter we discuss the important concepts of noetherian and artinian modules and rings. We begin with a very brief refresher on modules, before giving the definitions of noetherian and artinian modules, followed by examples. We conclude the chapter with a discussion of composition series and the Jordan–Hölder Theorem. In many places we follow the presentation in [Ash, §7.5]. Throughout this chapter, R denotes a ring. The notation $I \trianglelefteq R$ will denote that I is a (two-sided) ideal of R. For elements $a_1, \ldots, a_n \in R$, we denote the ideal generated by these elements by $\langle a_1, \ldots, a_n \rangle$.

1.1 Refresher on modules

We will very briefly review a few important concepts for modules. For further background on modules over rings, we refer the reader to [Ash, Ch. 4].

Recall that a *left module* over the ring R is an abelian group $(M, +)$ together with an action

$$R \times M \to M, \quad (r, m) \mapsto rm,$$

such that

$$r(x+y) = rx + ry, \quad (r+s)x = rx + sx, \quad r(sx) = (rs)x, \quad 1x = x,$$

for all $x, y \in M$ and $r, s \in R$. (Above, $1 = 1_R$ is the unit element of the ring R.) A *right module* over R is an abelian group $(M, +)$ together with an action

$$M \times R \to M, \quad (m, r) \mapsto mr,$$

such that

$$(x+y)r = xr + yr, \quad x(r+s) = xr + sx, \quad (xs)r = x(sr), \quad x1 = x,$$

for all $x, y \in M$ and $r, s \in R$. We will use the term *module* (or *R-module* when we wish to make the ring explicit) to mean left module.

If R is commutative, then the notions of left R-module and right R-module are equivalent. (See Exercise 1.2.1.) If R is a field, then an R-module is an R-vector space.

If M and N are R-modules, then $f\colon M \to N$ is a *module homomorphism* if f is a homomorphism of additive groups and

$$f(rm) = rf(m) \quad \text{for all } r \in R,\ m \in M.$$

The image $f(M)$ is a submodule of N, and the kernel $\ker f := f^{-1}(0)$ is a submodule of M. A *module isomorphism* is a bijective module homomorphism.

For R-modules M and N, we will use the notation $M \leq N$ or $N \geq M$ to indicate that M is a submodule of N.

Suppose N is a submodule of an R-module M. Then, in particular, N is an additive subgroup of M and thus we have the quotient group M/N (since the additive groups are commutative, all subgroups are normal). We define an R-module structure on M/N by

$$r(x + N) = rx + N, \quad r \in R,\ x \in M. \tag{1.1}$$

We leave it as Exercise 1.1.1 to verify that this action is well defined and endows M/N with the structure of an R-module.

Proposition 1.1.1 (Factor theorem for modules)**.** *Suppose $N \leq M$. Any module homomorphism $f\colon M \to L$ with $N \subseteq \ker f$ factors through M/N. In other words, there exists a unique module homomorphism*

$$\bar{f}\colon M/N \to L \quad \textit{such that} \quad \bar{f}(x + N) = f(x).$$

Furthermore:

(a) $\bar{f}$ is an epimorphism if and only if f is an epimorphism;

(b) $\bar{f}$ is a monomorphism if and only if $\ker f = N$.

Proof. The proof of this result is parallel to the corresponding result for groups or rings (see, for example, [Ash, 1.4.1, 2.3.1]) and so will be omitted. □

Theorem 1.1.2 (First isomorphism theorem for modules)**.** *If $f\colon M \to N$ is a module homomorphism, then $f(M) \cong M/(\ker f)$ as modules.*

Proof. This follows from Proposition 1.1.1 when we note that f is an epimorphism onto its image. □

Proposition 1.1.3 (Correspondence theorem for modules)**.** *Suppose N is a submodule of the R-module M. Then the map*

$$S \mapsto S/N$$

gives an inclusion-preserving one-to-one correspondence between the set of all submodules of M containing N and the set of all submodules of M/N.

Proof. By the correspondence theorem for groups (see, for example, [Ash, 1.4.6] or [Jud, Th. 11.13]), we have an inclusion-preserving one-to-one correspondence between additive subgroups of M containing N and additive subgroups of M/N. It remains to show that an additive subgroup S of M containing N is a *submodule* if and only if S/N is a submodule.

It is clear from the definition (1.1) of the action that if S is a submodule of M containing N, then S/N is a submodule of M/N. Now suppose that S is an additive subgroup of M containing N, such that S/N is a submodule of M/N. Let $x \in S$ and $r \in R$. Then $x + N \in S/N$, and so $rx + N \in S/N$. Hence, there exists $y \in S$ such that $rx + N = y + N$. Thus $rx - y \in N$, and so there exists some $z \in N$ such that $rx - y = z$. So

$$rx = y + z \in S + N = S,$$

since S contains N. □

Suppose M is an R-module. A *maximal proper submodule* of M is a proper submodule $N \subsetneq M$ such that

$$N \leq L \leq M \implies (N = L \text{ or } L = M).$$

A nonzero module is *simple* if it contains no proper nonzero submodules.

Lemma 1.1.4. *Suppose $N \leq M$. Then N is a maximal proper submodule of M if and only if M/N is simple.*

Proof. The proof of this lemma is left as Exercise 1.1.2. □

Suppose we have an R-module M_i for each i in some index set I. The *direct product* of the M_i, denoted $\prod_{i\in I} M_i$ consists of all families $(a_i)_{i\in I}$, where $a_i \in M_i$. The addition and action are defined by

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I}, \quad r(a_i)_{i\in I} = (ra_i)_{i\in I}.$$

The *(external) direct sum* of the M_i, denoted $\bigoplus_{i\in I} M_i$, is the submodule of $\prod_{i\in I} M_i$ consisting of those elements $(a_i)_{i\in I}$ such that $a_i = 0$ for all but finitely many i. For each $j \in I$, we have an injective module homomorphism

$$M_j \hookrightarrow \bigoplus_{i\in I} M_i, \quad a \mapsto (a_i)_{i\in i} \text{ where } a_i = \begin{cases} a & i = j, \\ 0 & i \neq j. \end{cases}$$

We will identify M_j with its image under this homomorphism and thus view M_j as a submodule of $\bigoplus_{i\in I} M_i$, and hence also of $\prod_{i\in I} M_i$.

If I is finite, then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$. If $I = \{1, 2, \ldots, n\}$, we often write the direct sum as

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Exercises.

1.1.1. Show that the action (1.1) is well-defined (that is, it is independent of the representative x of the coset $x + N$) and that this defines the structure of an R-module on M/N.

1.1.2. Prove Lemma 1.1.4.

1.1.3. Let k be a field and let $R = M_n(k)$ be the ring of $n \times n$ matrices with entries in k. Let $M = k^n$, considered as an R-module with action given by matrix multiplication. Prove that M is a simple R-module.

1.1.4. Suppose M and N are R-modules. Show that $(M \oplus N)/M \cong N$ as modules.

1.1.5. Suppose $N \leq L \leq M$ are R-modules. Then, by the correspondence theorem (Proposition 1.1.3), we have $L/N \leq M/N$. Prove that $M/L \cong (M/N)/(L/N)$. This is the *third isomorphism theorem* for modules.

1.1.6. Suppose M is an R-module. The *annihilator* of M is

$$\mathrm{Ann}_R(M) := \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

(a) Prove that $\mathrm{Ann}_R(M)$ is an ideal of R.

(b) Suppose I is an ideal of R and we try to define an action of R/I on M by

$$(r + I)m = rm, \quad r \in R,\ m \in M.$$

When is this action well defined?

1.2 Noetherian and artinian modules and rings

Let M be an R-module and suppose we have an increasing chain of submodules

$$M_1 \leq M_2 \leq M_3 \leq \cdots$$

or a decreasing chain of submodules

$$M_1 \geq M_2 \geq M_3 \geq \cdots .$$

We say that the chain *stabilizes* if there exists some t such that

$$M_t = M_{t+1} = M_{t+2} = \cdots .$$

The module M is said to satisfy the *ascending chain condition (ACC)* if every increasing chain of submodules stabilizes. Similarly, we say M satisfies the *descending chain condition (DCC)* if every decreasing sequence of submodules stabilizes.

Proposition 1.2.1. *For an R-module M, the following conditions are equivalent:*

(a) M satisfies the ACC;

(b) Every nonempty collection of submodules of M has a maximal element (with respect to inclusion).

Proof. Suppose (a) is satisfied, and let $\mathcal{S}$ be a nonempty collection of submodules. Choose $M_1 \in \mathcal{S}$. If M_1 is maximal, we are done. Otherwise, there exists some $M_2 \in \mathcal{S}$ with $M_1 \lneq M_2$. Continuing in this manner, we must eventually arrive at a maximal element; otherwise we could construct an infinite chain that does not stabilize, violating (a).

Conversely, suppose (b) is satisfied. Suppose we have an infinite chain

$$M_1 \leq M_2 \leq M_3 \leq \cdots$$

of submodules of M. If this chain did not stabilize, then $\{M_1, M_2, M_3, \dots\}$ would be a nonempty collection of submodules with no maximal element, contradicting (b). □

Proposition 1.2.2. *For an R-module M, the following conditions are equivalent:*

(a) M satisfies the DCC;

(b) Every nonempty collection of submodules of M has a minimal element (with respect to inclusion).

Proof. This proof, which is analogous to the proof of Proposition 1.2.1, is left as Exercise 1.2.2. □

Definition 1.2.3 (Noetherian module, artinian module)**.** An R-module satisfying the equivalent conditions of Proposition 1.2.1 is said to be *noetherian*. An R-module satisfying the equivalent conditions of Proposition 1.2.2 is said to be *artinian*.

Recall that, if N_1 and N_2 are submodules of M, then

$$N_1 + N_2 := \{x_1 + x_2 : x_1 \in N_1,\ x_2 \in N_2\}$$

is also a submodule of M.

Suppose S is a subset of an R-module M. We say that S *generates* M over R (or is a *generating set* for M over R) if every $x \in M$ can be written as a finite linear combination of elements of S with coefficients in R:

$$x = \sum_{i=1}^{n} r_i x_i, \quad r_1, \dots, r_n \in R,\ x_1, \dots, x_n \in S.$$

We say that M is *finitely generated* if it has a finite generating set. Thus, M is finitely generated if and only if there exist $x_1, \dots, x_n \in M$ such that

$$M = Rx_1 + Rx_2 + \cdots + Rx_n.$$

A module is *cyclic* if it is generated by a single element.

Proposition 1.2.4. *An R-module M is noetherian if and only if every submodule of M is finitely generated.*

Proof. First suppose that the ACC does not hold. Then there exists a sequence

$$M_1 \leq M_2 \leq M_3 \leq \cdots$$

of submodules of M that does not stabilize. Let $N = \bigcup_{r=1}^{\infty} M_r$. Then N is a submodule of M (Exercise 1.2.4). We claim that N is not finitely generated. Indeed, suppose, towards a contradiction that $x_1, \ldots, x_n$ generate N. Then there exists a sufficiently large t such that M_t contains all the x_i, which implies that $M_t = N$. Thus $M_t = M_{t+1} = \cdots$.

Conversely, suppose that the ACC holds, and let $N \leq M$. Choose $x_1 \in N$. If $Rx_1 = N$, then N is finitely generated. Otherwise, there exists $x_2 \notin Rx_1$. If the set $\{x_1, x_2\}$ generates N, we are done. Otherwise, there exists $x_3 \notin Rx_1 + Rx_2$. Continuing in this manner, we obtain a chain

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq Rx_1 + Rx_2 + Rx_3 \subsetneq \cdots .$$

The ACC forces this process to terminate at some stage. Thus there exists a t such that $x_1, \ldots, x_t$ generate N. □

Proposition 1.2.4 gives an alternative characterization of noetherian modules. There is an analogous statement for artinian rings. See Exercise 1.2.5.

Recall that every ring is a left module over itself with action given by the multiplication in the ring. Submodules correspond to left ideals. Similarly, every ring is a right module over itself, with submodules corresponding to right ideals.

Definition 1.2.5 (Noetherian ring, artinian ring)**.** A ring is *left noetherian* (resp. *right noetherian*) if is noetherian as a left (resp. right) module over itself. Similarly, a ring is *left artinian* (resp. *right artinian*) if is artinian as a left (resp. right) module over itself. For commutative rings, we simply use the terms *noetherian* and *artinian*.

Exercises.

1.2.1. For a ring R, the *opposite ring* R^{op} is the ring with the same underlying additive group, but with multiplication given by

$$r \cdot s = sr,$$

where $\cdot$ denotes the multiplication in R^{op} and juxtaposition denotes the multiplication in R. Prove that right R-modules are equivalent to left R^{op}-modules.

1.2.2. Prove Proposition 1.2.2.

1.2.3. (a) Is $\mathbb{Z}[x]$ finitely generated as a $\mathbb{Z}$-module?

(b) Is $\mathbb{Q}$ finitely generated as a $\mathbb{Z}$-module?

(c) Is $\mathbb{C}$ finitely generated as an $\mathbb{R}$-module?

Remember to justify your answers.

1.2.4. (a) Suppose $M_1 \leq M_2 \leq M_3 \leq \cdots$ is a chain of submodules of an R-module M. Prove that $\bigcup_{r=1}^{\infty} M_r$ is a submodule of M.

(b) Give an example of a ring R, an R-module M, and two submodules M_1 and M_2 such that $M_1 \cup M_2$ is *not* a submodule of M.

1.2.5 ([Ash, Prob. 7.5.8]). We say that an R-module L is *finitely cogenerated* if whenever the intersection of a collection of submodules of L is zero, then there is a finite subcollection whose intersection is zero. Show that a module M is artinian if and only if every quotient module M/N is finitely cogenerated.

1.2.6. Show that, for any ideal I of R, the R-module R/I is cyclic.

1.2.7 ([Ash, Prob. 7.5.6]). Let S be a subring of the ring R, and assume that S is a noetherian ring. If R is finitely generated as a module over S, show that R is also a noetherian ring.

1.3 Examples

Example 1.3.1. Every principal ideal domain (PID) is a noetherian ring. This follows immediately from Proposition 1.2.4 since every ideal is generated by a single element, by the definition of a PID.

Example 1.3.2. The ring $\mathbb{Z}$ of integers is noetherian (a special case of Example 1.3.1) but not artinian. For example,

$$\mathbb{Z} \supsetneq \langle 2 \rangle \supsetneq \langle 4 \rangle \supsetneq \langle 8 \rangle \supsetneq \cdots$$

is a descending chain that does not stabilize. We will see later that artinian rings are noetherian. (However, see Exercise 1.3.1.)

Suppose F is a field.

Example 1.3.3. The polynomial ring $F[X]$ is a PID, and hence is noetherian. (See, for example, [Sav, Th. 2.3.1].) However, the descending chain

$$\langle X \rangle \supsetneq \langle X^2 \rangle \supsetneq \langle X^3 \rangle \supsetneq \cdots$$

does not stabilize. Hence $F[X]$ is not artinian.

Example 1.3.4. The ring $F[X_1, X_2, \dots]$ of polynomials over F in infinitely many variables is neither artinian nor noetherian. Indeed,

$$\langle X_1 \rangle \supsetneq \langle X_1^2 \rangle \supsetneq \langle X_1^3 \rangle \supsetneq \cdots$$

is a descending chain that does not stabilize, and

$$\langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \cdots$$

is an ascending chain that does not stabilize.

So far, our examples of noetherian rings are all PIDs. After proving the Hilbert Basis Theorem (Theorem 2.2.1), we will be able to construct many more examples of noetherian rings, including ones which are not PIDs.

Exercises.

1.3.1 ([Ash, Prob. 7.5.1, 7.5.2]). Let p be a fixed prime, and let A be the abelian group of all rational numbers a/p^n, $n = \mathbb{Z}_{\geq 0}$, $a \in \mathbb{Z}$, under addition, where all calculations are modulo 1; in other words, A is a subgroup of $\mathbb{Q}/\mathbb{Z}$. Let A_n be the subgroup

$$\{0, 1/p^n, 2/p^n, \ldots, (p^n - 1)/p^n\}.$$

(a) Show that A is not a noetherian $\mathbb{Z}$-module.

(b) If B is a proper subgroup of A, show that B must be one of the A_n. Conclude that A is an artinian $\mathbb{Z}$-module.

(Note that this situation cannot arise for rings, where artinian implies noetherian.)

1.3.2 ([Ash, Prob. 7.5.7]). Let R be a ring, and assume that the polynomial ring $R[X]$ is noetherian. Does it follow that R is noetherian?

1.4 Composition series and the Jordan-Hölder Theorem

A common theme in mathematics is to reduce the study of some mathematical object to the study of simpler objects. For modules, this leads to the concept of a composition series, which we now explore. Our first result reduces the question of whether or not a given module is noetherian or artinian to the same question for smaller modules.

Proposition 1.4.1. *Suppose N is a submodule of an R-module M. Then M is noetherian (resp. artinian) if and only if N and M/N are both noetherian (resp. artinian).*

Proof. We will consider the artinian case, since the noetherian case is similar (see [Ash, Prop. 7.5.7]). Suppose M is artinian. Since any submodule of N is also a submodule of M, it follows that N is artinian by property (b) of Proposition 1.2.2. Now, by Proposition 1.1.3, every descending chain of submodules of M/N is of the form

$$M_1/N \geq M_2/N \geq \cdots \tag{1.2}$$

for some chain of submodules $M_1 \geq M_2 \geq \cdots$ of M. Since M is artinian, this chain stabilizes. Hence the chain (1.2) stabilizes. So M/N is artinian.

Conversely, suppose M and M/N are artinian. Let

$$M_1 \geq M_2 \geq \cdots \tag{1.3}$$

be a decreasing sequence of submodules of M. Then

$$M_1 \cap N \geq M_2 \cap N \geq \cdots \tag{1.4}$$

is a decreasing sequence of submodules of N, and

$$M_1 + N \geq M_2 + N \geq \cdots$$

is a decreasing sequence of submodules of M containing N. Hence

$$(M_1 + N)/N \geq (M_2 + N)/N \geq \cdots \tag{1.5}$$

is a decreasing sequence of submodule of M/N. Since M and M/N are both noetherian, we can choose i large enough such that the sequences (1.4) and (1.5) have stabilized. That is, we have

$$M_i \cap N = M_{i+1} \cap N = \cdots \quad \text{and} \quad (M_i + N)/N = (M_{i+1} + N)/N = \cdots .$$

By Proposition 1.1.3, we also have

$$M_i + N = M_{i+1} + N = \cdots .$$

We claim that the sequence (1.3) also stabilizes at the i-th term. So we want to show that $M_i = M_j$ for all $j \geq i$. Suppose $j \geq i$ and $x \in M_i$. Then

$$x + N \in M_i + N = M_j + N,$$

and so $x + N = y + N$ for some $y \in M_j \subseteq M_i$. Therefore

$$x - y \in M_i \cap N = M_j \cap N.$$

Thus, there exists some $z \in M_j \cap N$ such that $x - y = z$, which implies that

$$x = y + z \in M_j.$$

This implies that $M_i = M_j$, and desired. □

Corollary 1.4.2. *If $M_1, \ldots, M_n$ are noetherian (resp. artinian) R-modules, then so is $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.*

Proof. It suffices to consider the case $n = 2$, since then the general result follows by induction. By hypothesis,

$$M_1 \quad \text{and} \quad (M_1 \oplus M_2)/M_1 \cong M_2$$

are noetherian (resp. artinian) by hypothesis. (For the isomorphism, see Exercise 1.1.4.) Then the result follows from Proposition 1.4.1. □

Definition 1.4.3 (Composition series)**.** A *series* of *length* n for a module M is a sequence of submodules of the form

$$M = M_0 \gneq M_1 \gneq \cdots \gneq M_n = 0.$$

The series is a *composition series* if each factor M_i/M_{i+1}, $0 \leq i \leq n-1$, is simple. Two series are *equivalent* if they have the same length and the same factor modules, up to isomorphism and reordering.

By convention, the zero module has a composition series of length zero, namely 0 itself.

Theorem 1.4.4 (Jordan–Hölder Theorem)**.** *If M has a composition series, then any two composition series for M are equivalent. Furthermore, any strictly decreasing sequence of submodules can be refined to a composition series.*

Proof. The proof of this theorem is almost identical to the proof of the Jordan–Hölder Theorem for groups, which is proved in MAT 5142 (Algebra II). (See, for example, [Ash, §5.6.6, §7.5.11].) Thus, we will omit its proof here. □

We think of the factor modules in a composition series for M as building blocks for M. The Jordan–Hölder Theorem states that these building blocks are unique *if* they exist (i.e. if M has a composition series). The next result tells us when a module has a composition series.

Theorem 1.4.5. *A module has a composition series if and only if it is both noetherian and artinian.*

Proof. Suppose a module M has a composition series of length n. If M is not noetherian or not artinian, we can find an infinite sequence of submodules that does not stabilize. Throwing out some submodules, we can construct a series for M of length $n+1$. By the Jordan–Hölder Theorem, we can refine this to a composition series, which must have length n. But refining a series increases its length, so this is a contradiction.

Now assume that M is noetherian and artinian. If $M = 0$, it has a composition series and we are done. Thus, suppose $M \neq 0$. Applying condition (b) of Proposition 1.2.1 to the set of all proper submodules of M, we can choose a maximal proper submodule M_1 of M. By Proposition 1.4.1, M_1 is also noetherian. Thus, if $M_1 \neq 0$, then M_1 has a maximal proper submodule M_2. Continuing in this manner, we construct a sequence

$$M = M_0 \geq M_1 \geq M_2 \geq \cdots .$$

We must eventually reach zero (that is, $M_n = 0$ for some n) since M is artinian. Because each M_{i+1} is a maximal submodule of M_i, for $0 \leq i \leq n-1$, each factor M_i/M_{i+1} is simple by Lemma 1.1.4. Thus we have constructed a composition series for M. □

Exercises.

1.4.1. Suppose $M_1, \ldots, M_n$ are simple R-modules. Give a composition series for $M_1 \oplus M_2 \oplus \cdots \oplus M_n$. Don't forget to justify your answer.

1.4.2. Suppose I is an index set and M_i is a simple R-module for each $i \in I$. Prove that the following statements are equivalent:

(a) $\bigoplus_{i \in I} M_i$ is noetherian;

(b) $\bigoplus_{i \in I} M_i$ is artinian;

(c) The set I is finite.

1.4.3 ([Ash, Prob. 7.5.3]). Suppose V is a vector space (that is, it is a module over a field). Prove that the following statements are equivalent:

(a) V is finite dimensional;

(b) V is noetherian;

(c) V is artinian;

(d) V has a composition series.

Hint: Use Exercise 1.4.2.

1.4.4. Consider the ring $R = \mathbb{C}[X]$ and let n be a positive integer. Give a composition series for the R-module $\mathbb{C}[X]/\langle X^n \rangle$ (with the action induced by multiplication). *Hint*: Use the third isomorphism theorem for modules (see Exercise 1.1.5 or [Ash, §4.2.4]).

1.4.5 ([Ash, Prob. 7.5.4, 7.5.5]). Define the *length* of a module M, denoted $\ell(M)$, to be the length of a composition series. If M has no composition series, we set $\ell(M) = \infty$. Suppose that $N \leq M$.

(a) Prove that $\ell(M)$ is finite if and only if $\ell(N)$ and $\ell(M/N)$ are finite.

(b) If $\ell(M)$ is finite, show that $\ell(M) = \ell(N) + \ell(M/N)$.

1.4.6. Let A be a noetherian (respectively, artinian) ring and suppose I is an ideal of A. Prove that A/I is a noetherian (respectively, artinian) ring.

Chapter 2

Commutative algebra

Through this chapter, k will denote a field. The material in this chapter roughly corresponds to [Ash, Ch. 8], except for Section 2.4, which follows [Ash, §7.1]

2.1 Affine varieties

Definition 2.1.1 (Affine n-space, affine variety)**.** For $n \in \mathbb{Z}_{>0}$, the set

$$\mathbb{A}^n = \mathbb{A}^n(k) = \{(a_1, a_2, \ldots, a_n) : a_1, \ldots, a_n \in k\}$$

is called *affine n-space*. If $S \subseteq k[X_1, \ldots, X_n]$ is a set of polynomials, then the zero set

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

of S is called an *affine variety*. Since this is the only type of variety will we encounter in this course, we will also simply call it a *variety*. Thus, a variety is the solution set of a system of polynomial equations.

Suppose $S \subseteq k[X_1, \ldots, X_n]$, and let I be the ideal generated by S. Since $S \subseteq I$, we have $V(I) \subseteq V(S)$. Note also that I consists of linear combinations of the form

$$\sum_{i=1}^{m} g_i f_i, \quad g_i \in k[X_1, \ldots, X_n], \ f_i \in S.$$

Thus we also have $V(S) \subseteq V(I)$; hence $V(S) = V(I)$. So every variety is the variety of some *ideal*.

Recall that if $I_1, \ldots, I_r$ are ideals of some commutative ring, then

$$\prod_{j=1}^{r} I_j = I_1 I_2 \cdots I_r = \left\{ \sum_{i=1}^{m} a_{1,i} a_{2,i} \cdots a_{r,i} : m \in \mathbb{N}, \ a_{j,i} \in I_j \text{ for all } i, j \right\}.$$

It follows that

$$\prod_{j=1}^{r} I_j \subseteq \bigcap_{j=1}^{r} I_j. \tag{2.1}$$

Note that the inclusion may be strict. (See Exercise 2.1.1.)

Proposition 2.1.2. *(a) Suppose $I_\alpha \trianglelefteq k[X_1, \dots, X_n]$ for each α in some index set T. Then*

$$\bigcap_{\alpha \in T} V(I_\alpha) = V\left(\bigcup_{\alpha \in T} I_\alpha\right).$$

In particular, an arbitrary intersection of varieties is a variety.

(b) If $I_1, \dots, I_r \trianglelefteq k[X_1, \dots, X_n]$, then

$$\bigcup_{j=1}^{r} V(I_j) = V\left(\prod_{j=1}^{r} I_j\right) = V\left(\bigcap_{j=1}^{r} I_j\right).$$

In particular, a finite *union of varieties is a variety.*

(c) We have $\mathbb{A}^n = V(0)$ and $\varnothing = V(1)$. In particular, the empty set $\varnothing \subseteq \mathbb{A}^n$ and $\mathbb{A}^n$ itself are varieties.

Proof. (a) For $x \in \mathbb{A}^n$, we have

$$\begin{aligned} x \in \bigcap_{\alpha \in T} V(I_\alpha) &\iff f(x) = 0 \text{ for all } f \in I_\alpha,\ \alpha \in T \\ &\iff x \in V\left(\bigcup_{\alpha \in T} I_\alpha\right). \end{aligned}$$

(b) For $x \in \mathbb{A}^n$, we have

$$\begin{aligned} x \in \bigcup_{j=1}^{r} V(I_j) &\iff \exists\, j \in \{1, \dots, r\} \text{ such that } (f(x) = 0\ \forall\ f \in I_j) \\ &\iff (f_1 \cdots f_r)(x) = 0 \text{ for all } f_j \in I_j,\ j \in \{1, \dots, r\} \\ &\iff x \in V\left(\prod_{j=1}^{r} I_j\right). \end{aligned}$$

Now, the (2.1) implies that

$$V\left(\bigcap_{j=1}^{r} I_j\right) \subseteq V\left(\prod_{j=1}^{r} I_j\right).$$

To see the reverse inclusion, suppose $x \in V\left(\prod_{j=1}^{r} I_j\right)$ and $f \in \bigcap_{j=1}^{r} I_j$. Then $f^r \in \prod_{j=1}^{r} I_j$, and so $f(x)^r = 0$, which implies that $f(x) = 0$. (Here we use the fact that k is a field, hence has no nonzero zero divisors.)

(c) This is clear.

□

Proposition 2.1.2 implies that the collection of varieties satisfies the axioms of closed subsets of a topology. Equivalently, the collection of complements of varieties satisfy the axioms of open subsets of a topology. This topology on $\mathbb{A}^n$ is called the *Zariski topology*.

Above we have associated a subset of $\mathbb{A}^n$ to every ideal of $k[X_1, \dots, X_n]$. Now we do the opposite.

Definition 2.1.3 (Ideal of a subset)**.** Suppose $X \subseteq \mathbb{A}^n$ is an arbitrary subset. The *(vanishing) ideal* of X is

$$I(X) = \{f \in k[X_1, \ldots, X_n] : f(x) = 0 \text{ for all } x \in X\}.$$

We leave it as Exercise 2.1.2 to verify that $I(X)$ is indeed an ideal of $k[X_1, \ldots, X_n]$.

We will write $IV(S)$ for $I(V(S))$ and $IVI(X)$ for $I(V(I(X)))$, etc.

Proposition 2.1.4. *Suppose $X, Y \subseteq \mathbb{A}^n$ and $S, T \subseteq k[X_1, \ldots, X_n]$.*

(a) If $X \subseteq Y$, then $I(X) \supseteq I(Y)$.

(b) If $S \subseteq T$, then $V(S) \supseteq V(T)$.

(c) We have $IV(S) \supseteq S$ and $VI(X) \supseteq X$.

(d) We have $VIV(S) = V(S)$ and $IVI(X) = I(X)$.

Proof. (a) This is clear from the definitions.

(b) This is also clear from the definitions.

(c) If $f \in S$, then $f(x) = 0$ for all $x \in V(S)$, and so $f \in IV(S)$. If $x \in X$, then $f(x) = 0$ for all $f \in I(X)$, and so $x \in VI(X)$.

(d) By (c), we have $IV(S) \supseteq S$. Hence, by (b), we have $VIV(S) \subseteq V(S)$. Now, for $x \in V(S)$ and $f \in IV(S)$, we have $f(x) = 0$, and so $x \in VIV(S)$. This gives us the reverse inclusion $V(S) \subseteq VIV(S)$.

Similarly, by (c), we have $VI(X) \supseteq X$. Hence, by (a), we have $IVI(X) \subseteq I(X)$. Now, for $f \in I(X)$ and $x \in VI(X)$, we have $f(x) = 0$, and so $f \in IVI(X)$. This gives us the reverse inclusion $I(X) \subseteq IVI(X)$.

□

If $a_1, \ldots, a_r$ are elements of R, then we let

$$\langle a_1, \ldots, a_r \rangle \trianglelefteq R$$

denote the ideal of R generated by these elements.

Proposition 2.1.5. *(a) We have $I(\varnothing) = k[X_1, \ldots, X_n]$.*

(b) If k is an infinite field, then $I(\mathbb{A}^n) = \{0\}$.

(c) If $x = (a_1, \ldots, a_n) \in \mathbb{A}^n$, then $I(\{x\}) = \langle X - a_1, \ldots, X - a_n \rangle$.

Proof. (a) This is clear.

(b) Suppose k is an infinite field. We prove that $I(\mathbb{A}^n) = \{0\}$ by induction on n. The result holds for $n = 1$ since a nonconstant polynomial in one variable has only finitely many zeros. Thus $f \neq 0$ implies that $f \notin I(\mathbb{A}^1)$.

Now suppose $n > 1$ and that the result holds for $n - 1$. Let $f \in k[X_1, \ldots, X_n]$. Then we can write

$$f = g_r X_n^r + \ldots + g_1 X_n + g_0, \quad g_0, \ldots, g_r \in k[X_1, \ldots, X_{n-1}],\ g_r \neq 0.$$

By the induction hypothesis, there is a point $(x_1, \ldots, x_{n-1}) \in \mathbb{A}^{n-1}$ at which g_r does not vanish. Then

$$f(x_1, \ldots, x_{n-1}, X_n) \in k[X_n]$$

is a nonzero polynomial which cannot vanish at all $x_n \in k$. Hence $f \notin I(\mathbb{A}^n)$.

(c) It is clear that

$$\langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq I(\{x\})$$

since $X_i - a_i$ vanishes at x for each $i \in \{1, \ldots, n\}$. We prove the reverse inclusion by induction on n. The result holds for $n = 1$ by the remainder theorem (see [Ash, §2.5.2]). Now suppose $n > 1$ and that the result holds for $n - 1$. Let $f \in I(\{x\})$. As above, we can write

$$f = g_r X_n^r + \ldots + g_1 X_n + g_0, \quad g_0, \ldots, g_r \in k[X_1, \ldots, X_{n-1}],\ g_r \neq 0.$$

By the division algorithm (see [Ash, §2.5.1]), we have

$$f = (X_n - a_n) g(X_1, \ldots, X_n) + h(X_1, \ldots, X_{n-1}),$$

and h must vanish at $(a_1, \ldots, a_{n-1})$. By the induction hypothesis, $h \in \langle X_1 - a_1, \ldots, X_{n-1} - a_{n-1} \rangle$, and so $f \in \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

□

If $X \subseteq \mathbb{A}^n$, then each polynomial $f \in k[X_1, \ldots, X_n]$ defines a function $f \colon X \to k$. Two polynomials define the same function precisely when their difference lies in $I(X)$. This leads to the following definition.

Definition 2.1.6 (Coordinate ring)**.** If $V \subseteq \mathbb{A}^n$ is a variety, then we call $k[X_1, \ldots, X_n]/I(V)$ the *coordinate ring* of V.

Exercises.

2.1.1. Give an example of a ring R with ideals I and J such that $IJ \subsetneq I \cap J$.

2.1.2. Suppose $X \subseteq \mathbb{A}^n$. Prove that $I(X)$ is an ideal of $k[X_1, \ldots, X_n]$.

A variety is *reducible* if it is a union of two proper subvarieties. If a variety is not reducible, then it is *irreducible*. In Exercises 2.1.3 to 2.1.6, we will show that a variety V is irreducible if and only if $I(V)$ is a prime ideal.

2.1.3 ([Ash, Prob. 8.1.1]). Assume that $I(V)$ is not prime, and let $f_1, f_2 \in I(V)$ with $f_1, f_2 \notin I(V)$. If $x \in V$, show that

$$x \notin V(f_1) \implies x \in V(f_2).$$

(Hence $x \notin V(f_2) \implies V(f_1)$.)

2.1.4 ([Ash, Prob. 8.1.2]). Assume that $I(V)$ is not prime. Show that V is reducible.

2.1.5 ([Ash, Prob. 8.1.3]). Show that if V and W are varieties with $V \subsetneq W$, then $I(V) \supsetneq I(W)$.

2.1.6 ([Ash, Prob. 8.1.4]). Assume that V_1, V_2, V are varieties with $V = V_1 \cup V_2$, $V_1, V_2 \subsetneq V$. By Exercise 2.1.5, we can choose $f_i \in I(V_i)$ with $f_i \notin I(V)$ for $i = 1, 2$. Show that $f_1 f_2 \in I(V)$, so $I(V)$ is not a prime ideal.

2.1.7 ([Ash, Prob. 8.1.5, 8.1.6]). Show that any variety is the union of finitely many irreducible subvarieties. Furthermore, show that this decomposition is unique if we impose the condition that none of the subvarieties is contained in any of the others.

2.1.8 ([Ash, Prob. 8.1.7]). Assume that k is algebraically closed. Suppose that $\mathbb{A}^n$ is covered by open sets $\mathbb{A}^n \setminus V(I_i)$ in the Zariski topology (i.e. $\mathbb{A}^n = \bigcup_i (\mathbb{A}^n \setminus V(I_i))$). Let I be the ideal generated by the I_i, so that $I = \sum_i I_i$, the set of all finite sums $x_{i_1} + \ldots + x_{i_r}$, with $x_{i_j} \in I_{i_j}$. Show that $1 \in I$. You may use the weak Nullstellensatz (see Theorem 2.6.1(b)).

2.1.9 ([Ash, Prob. 8.1.8]). Recall that a subset of a topological space is *compact* if any open cover has a finite subcover. Show that $\mathbb{A}^n$ is compact in the Zariski topology. In other words, show that if

$$\mathbb{A}^n = \bigcup_{\alpha \in T} (\mathbb{A}^n \setminus V(I_\alpha))$$

for some $I_\alpha \trianglelefteq k[X_1, \ldots, X_n]$, with α ranging over a (possibly infinite) index set T, then there is a finite subset $T' \subseteq T$ such that

$$\mathbb{A}^n = \bigcup_{\alpha \in T'} (\mathbb{A}^n \setminus V(I_\alpha))$$

2.2 The Hilbert Basis Theorem

We have seen that a set of polynomial equations defines a variety. In particular, to a subset S of $k[X_1, \ldots, X_n]$, we have associated the variety $V(S)$. We saw that this variety is also equal to $V(I)$, where I is the ideal generated by S. In general, the set S may be infinite. However, it turns out that every variety is equal to $V(S)$ for some *finite* set S. This follows from the fact (to be proved) that every ideal of $k[X_1, \ldots, X_n]$ is finitely generated. In other words, the ring $k[X_1, \ldots, X_n]$ is noetherian. This is a corollary of the following result.

Theorem 2.2.1 (Hilbert Basis Theorem)**.** *If R is a noetherian ring, then the ring $R[X_1, \ldots, X_n]$ is also noetherian.*

Proof. Since $R[X_1, X_2] \cong (R[X_1])[X_2]$, etc. it suffices to prove the result for $n = 1$. Then the result for general n will follow by induction. So we need to show that every ideal of $R[X]$ is finitely generated.

Let $I \trianglelefteq R[X]$. Let J be the set of all leading coefficients of elements of I. (By convention, the leading coefficient of the zero polynomial is 0.) It is straightforward to verify that $J \trianglelefteq R$. Thus, since R is noetherian, J is finitely generated. Let $a_1, \ldots, a_n$ be a set of generators of J. For each $i = 1, \ldots, n$, let $f_i \in I$ be a polynomial with leading coefficient a_i, and let d_i be the degree of f_i.

Let $d = \max\{d_i : 1 \leq i \leq n\}$, and define

$$I^* = \{f \in I : \deg f \leq d\}.$$

Consider the R-module

$$M := \{b_d X^d + \cdots + b_1 X + b_0 : b_i \in R\}.$$

The map

$$M \to R^{d+1}, \quad b_d X^d + \cdots + b_0 \mapsto (b_d, \ldots, b_0),$$

is an isomorphism of R-modules. The assumption that R is a noetherian ring means precisely that R is a noetherian R-module. Hence, by Corollary 1.4.2, R^{d+1} is a noetherian R-module. Thus M is a noetherian R-module. Since I^* is a submodule of M, this implies that I^* is finitely generated.

Let $g_1, \ldots, g_m$ be a set of generators of I^* and set

$$I_0 = \langle f_1, \ldots, f_n, g_1, \ldots, g_m \rangle \trianglelefteq R[X].$$

We will show that $I_0 = I$, which implies that I is finitely generated, as desired.

Since $f_i \in I$ and $g_j \in I^* \subseteq I$ for all i, j, we have $I_0 \subseteq I$. So it remains to prove the reverse inclusion. Let $h \in I$. We wish to show that $h \in I_0$, which we do by induction on the degree of h.

First suppose $\deg h \leq d$. Then $h \in I^*$, and so h is an R-linear combination (hence also an $R[X]$-linear combination) of the g_j. So $h \in I_0$.

Now suppose that $\deg h = r > d$ and that all elements of I of degree less than r are contained in I_0. Let a be the leading coefficient of h. Thus $a \in J$, and so $a = \sum_{i=1}^n c_i a_i$ for some $c_1, \ldots, c_n \in R$. Let

$$q = h - \sum_{i=1}^n c_i X^{r-d_i} f_i \in I.$$

The coefficient of X^r in q is

$$a - \sum_{i=1}^n c_i a_i = 0.$$

Thus $\deg q < r$. By our induction hypothesis, $q \in I_0$. Thus

$$h = q + \sum_{i=1}^n c_i X^{r-d_i} f_i \in I_0,$$

completing the proof of the induction step. □

A *hypersurface* is the zero-set zero of a single polynomial. In other words, a hypersurface is a variety of the form $V(f)$ for some $f \in k[X_1, \ldots, X_n]$.

Corollary 2.2.2. *Every variety is the intersection of finitely many hypersurfaces.*

Proof. Let $V = V(I)$ be a variety. By the Hilbert Basis Theorem (Theorem 2.2.1), I has a finite set $f_1, \ldots, f_n$ of generators. Then

$$V(I) = V(\{f_1, \ldots, f_n\}) = \bigcap_{i=1}^{n} V(f_i),$$

by Proposition 2.1.2(a). □

Remark 2.2.3. One can adapt the proof of the Hilbert Basis Theorem (Theorem 2.2.1) to show that if R is noetherian, then the ring $R[\![X]\!]$ of formal power series is noetherian. One must look at terms of *lowest* degree instead of highest degree. See [Ash, §8.2.3] for details.

Exercises.

2.2.1. If $a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ is a nonzero polynomial in $R[X]$ with $a_n \neq 0$, then a_n is called the *leading coefficient* of the polynomial. By convention, the leading coefficient of the zero polynomial is 0. Suppose $I \trianglelefteq R[X]$, and let J be the set of all leading coefficients of elements of I. Show that $I \trianglelefteq R$.

2.2.2 ([Ash, Prob. 8.2.4, 8.2.5]). Let R be a subring of S, and assume that S is finitely generated as an algebra over R. In other words, there are finitely many elements $x_1, \ldots, x_n \in S$ such that the smallest subring of S containing all the x_i and all elements of R is S itself.

(a) Show that S is a homomorphic image of the polynomial ring $R[X_1, \ldots, X_n]$ (i.e. it is the image of some ring homomorphism with domain $R[X_1, \ldots, X_n]$).

(b) Show that if R is noetherian, then S is also noetherian.

2.3 Radical ideals

We have defined maps

$$\text{varieties in } \mathbb{A}^n \underset{V}{\overset{I}{\rightleftarrows}} \text{ideals of } k[X_1, \ldots, X_n]. \tag{2.2}$$

Since, by definition, a variety is a set of the form $V(S) \subseteq \mathbb{A}^n$, it follows from Proposition 2.1.4(d) that, for varieties $V_1 = V(S_1)$ and $V_2 = V(S_2)$,

$$I(V_1) = I(V_2) \implies V_1 = V(S_1) = VIV(S_1) = VIV(S_2) = VIV(S_2) = V(S_2) = V_2.$$

In other words, the map I in (2.2) is injective.

On the other hand, the map V in (2.2) is certainly *not* injective. For instance, for $f \in k[X_1, \ldots, X_n]$, it is possible that $\langle f \rangle \neq \langle f^m \rangle$ when $m > 1$, but $V(f) = V(f^m)$. While it seems that the two statements in Proposition 2.1.4(d) are symmetric in V and I, there is a subtle difference. A variety is, by definition, a set of the form $V(S)$, while it is not the case that every ideal of $k[X_1, \ldots, X_n]$ is of the form $I(V)$ for some variety V.

To remedy the above problem, we need to determine which types of ideals are of the form $I(V)$ for some variety V or, equivalently, to know precisely what types of ideals can define the same variety. Hilbert's Nullstellensatz says that if two ideals define the same variety, then they are the same "up to powers": if f belongs to one of the ideals, then f^r belongs to the other for some positive integer r.

In this section, we will build up some results needed to prove the Nullstellensatz. The first shows that points correspond to maximal ideals.

Lemma 2.3.1. *If $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$, then $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ is a maximal ideal.*

Proof. Let $I = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ and suppose I is properly contained in $J \trianglelefteq k[X_1, \ldots, X_n]$. Choose $f \in J \setminus I$. Since $k[X_1, \ldots, X_n] = k[X_2, \ldots, X_{n-1}][X_1]$, we can use the division algorithm to write

$$f = g_1(X_1 - a_1) + h_1,$$

where $g_2 \in k[X_1, \ldots, X_n]$ and $h_1 \in k[X_2, \ldots, X_n]$ (i.e. we can choose the remainder h to have degree zero in X_1 since we are dividing by $X_1 - a_1$, which has degree one in X_1). Using the division algorithm on $h_1 \in k[X_3, \ldots, X_n][X_2]$, we can write

$$f = g_1(X_1 - a_1) + g_2(X_2 - a_2) + h_2, \quad g_2 \in k[X_2, \ldots, X_n],\ h_2 \in k[X_3, \ldots, X_n].$$

Continuing in this manner, we can write

$$\begin{aligned} f = g_1(X_1 - a_1) + g_2(X_2 - a_2) + \ldots + g_n(X_n - a_n) + b, \quad \text{where} \\ g_1 \in k[X_1, \ldots, X_n],\ g_2 \in k[X_2, \ldots, X_n], \ldots, g_n \in k[X_n],\ b \in k. \end{aligned} \tag{2.3}$$

Since $f \notin I$, we have $b \neq 0$. However, since $f \in J$, we can solve (2.3) for b to see that $b \in J$. Hence $1 = \frac{1}{b} b \in J$, and so $J = k[X_1, \ldots, X_n]$. It follows that the ideal I is maximal. □

Definition 2.3.2 (Radical of an ideal)**.** Suppose I is an ideal of a commutative ring R. The *radical* of I is

$$\sqrt{I} := \{f \in R : f^r \in I \text{ for some } r \in \mathbb{Z}_{>0}\}.$$

An ideal is a *radical ideal* if $\sqrt{I} = I$.

Note that $\sqrt{I}$ is, in fact, an ideal. If $f, g \in \sqrt{I}$, then $f^r, g^s \in I$ for some $r, s \in \mathbb{Z}_{>0}$. Then, by the binomial theorem,

$$(f+g)^{r+s-1} = \sum_{i=0}^{r+s-1} f^i g^{r+s-1-i} \in I.$$

Also, for $h \in k[X_1, \ldots, X_n]$, we have $(fh)^r = f^r h^r \in I$.

Lemma 2.3.3. *If $I \trianglelefteq k[X_1, \ldots, X_n]$, then $\sqrt{I} \subseteq IV(I)$.*

Proof. Suppose $f \in \sqrt{I}$. Then there exists $r \in \mathbb{Z}_{>0}$ such that $f^r \in I$. Thus, for all $x \in V(I)$, we have $f^r(x) = 0$, which implies that $f(x) = 0$. So $f \in IV(I)$. □

The Nullstellensatz states that $IV(I) = \sqrt{I}$. The hard part is to prove that $IV(I) \subseteq \sqrt{I}$.

Exercises.

2.3.1. Suppose I and J are ideals of some commutative ring R. Prove the following:

(a) $\sqrt{\sqrt{I}} = \sqrt{I}$

(b) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

(c) $\sqrt{I} = R$ if and only if $I = R$

(d) If P is a prime ideal of R, then $\sqrt{P^n} = P$ for all $n > 0$.

2.3.2. Let I be an ideal of a commutative ring R. Show that if $\sqrt{I}$ is finitely generated then $\left(\sqrt{I}\right)^r \subseteq I$ for some positive integer r.

2.3.3. Suppose I and J are ideals of a commutative noetherian ring. Show that I and J have the same radical if and only if I contains some power of J and J contains some power of I.

2.3.4. Let I be an ideal of a commutative ring R. Recall that $a \in R$ is *nilpotent* if $a^m = 0$ for some positive integer m. Show that

$$\sqrt{I} = \{a \in R : a + I \text{ is a nilpotent element of } R/I\}.$$

2.3.5 ([Ash, 8.3.1]). A subset S of a ring R is *multiplicative* if $0 \notin S$, $1 \in S$, and whenever $a, b \in S$, we have $ab \in S$. Let S be a multiplicative subset of the ring R. If I is an ideal that is disjoint from S, then by Zorn's lemma, there is an ideal J that is maximal among ideals disjoint from S. Show that J must be prime.

2.3.6 ([Ash, 8.3.2]). Show that the radical of the ideal I is the intersection of all prime ideals containing I. *Hint*: If $f^r \in I \subseteq P$, with P a prime ideal, then $f \in P$. Conversely, assume $f \in \sqrt{I}$. With a clever choice of multiplicative set S, show that for some prime ideal P containing I, we have $f \notin P$.

2.3.7 ([Ash, 8.3.4]). Show that the variety $V \subseteq \mathbb{A}^3$ defined over the complex numbers by the two polynomials $Y^2 - XZ$ and $Z^2 - X^2Y$ is the union of the line $L = \{(x, 0, 0) : x \in \mathbb{C}\}$ and the set $W = \{(t^3, t^4, t^5) : t \in \mathbb{C}\}$.

2.3.8 ([Ash, 8.3.4]). The *twisted cubic* is the variety V defined over the complex numbers by $Y - X^2$ and $Z - X^3$. In parametric form, $V = \{(t, t^2, t^3) : t \in \mathbb{C}\}$. Show that the V is irreducible. *Hint*: Show that $I(V)$ is a prime ideal. (The same argument works for any variety that can be parameterized over an infinite field.)

2.4 Integral extensions

Before proving the Nullstellensatz, we need a slight digression about rings. We follow the presentation in [Ash, §7.1]. In this section *all rings are commutative*.

Suppose A is a subring of a ring R. We say that $x \in R$ is *integral* over A if x is a root of a monic polynomial with coefficients in A. We say that R is integral over A if every element of R is integral over A.

Example 2.4.1. An *algebraic integer* is a real or complex number that is integral over $\mathbb{Z}$. For example, for every $d \in \mathbb{Z}$, $\sqrt{d}$ is an algebraic integer, since it is a root of the monic polynomial $X^2 - d$. Similarly, every n-th root of unity is an algebraic integer.

If $x_1, \ldots, x_n \in R$, then

$$A[x_1, \ldots, x_n] = \{f(x_1, \ldots, x_n) : f \in A[X_1, \ldots, X_n]\} \subseteq R$$

is the subring of R consisting of all elements of R that can be expressed as a polynomial in the x_i, with coefficients in R. Note that this is different than the polynomial ring $A[X_1, \ldots, X_n]$, since the x_i are not necessarily indeterminates. In addition to being a ring, $A[x_1, \ldots, x_n]$ is also naturally an A-module.

Proposition 2.4.2. *Suppose A is a subring of R, with $x \in R$. The following conditions are equivalent.*

(a) x is integral over A;

(b) The A-module $A[x]$ is finitely generated;

(c) x belongs to a subring B of R such that $A \subseteq B$ and B is a finitely generated A-module.

Proof. (a) $\implies$ (b): If x is a root of a monic polynomial over A of degree n, then x^d, $d \geq n$, can be written as a linear combination of lower powers of x. Hence $1, x, x^2, \ldots, x^{n-1}$ generate $A[x]$ over A.

(b) $\implies$ (c): Simply take $B = A[x]$.

(c) $\implies$ (a): Suppose $y_1, \ldots, y_n$ generate B as an A-module. Then xy_i is a linear combination of the y_j, so we can write

$$xy_i = \sum_{j=1}^{n} c_{i,j} y_j, \quad c_{i,j} \in A.$$

So if y is the column vector with components $y_1, \ldots, y_n$, I is the $n \times n$ identity matrix, and $C = [c_{i,j}]$, we have

$$(xI - C)y = 0.$$

It follows that x is a root of the monic polynomial $\det(XI - C)$ in $A[X]$. □

Lemma 2.4.3. *Suppose A is a subring of R, with $x_1, \ldots, x_n \in R$. If x_1 is integral over A, x_2 is integral over $A[x_1]$, ..., and x_n is integral over $A[x_1, \ldots, x_{n-1}]$, then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Proof. We prove the result by induction on n. The case $n = 1$ follows from Proposition 2.4.2.

Now suppose $n > 1$ and that the result holds for $n - 1$. Consider the extensions

$$A \subseteq A[x_1, \ldots, x_{n-1}] \subseteq A[x_1, \ldots, x_n] = \big(A[x_1, \ldots, x_{n-1}]\big)[x_n].$$

By the induction hypothesis, $A[x_1, \ldots, x_n]$ is finitely generated as an A-module. Also, by the $n = 1$ case, $A[x_1, \ldots, x_n]$ is finitely generated as an $A[x_1, \ldots, x_{n-1}]$-module.

To complete the proof of the induction step, it suffices to prove that if $A \subseteq B \subseteq C$ are rings, with C a finitely generated B-module and B a finitely generated C-module, then C is a finitely generated A-module. To see this, note that if

$$C = \sum_{j=1}^{r} By_j \quad \text{and} \quad B = \sum_{k=1}^{s} Az_k,$$

then

$$C = \sum_{j=1}^{r} \sum_{k=1}^{s} Ay_j z_k. \qquad \square$$

Proposition 2.4.4 (Transitivity of integral extensions)**.** *Suppose A, B, and C are subrings of R. If C is integral over B, and B is integral over A, then C is integral over A.*

Proof. Let $x \in C$. Since C is integral over B, we have

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0 \quad \text{for some } b_0, \ldots, b_{n-1} \in B.$$

Then x is integral over $A[b_0, \ldots, b_{n-1}]$. Since B is integral over A, each b_i is integral over A, hence over $A[b_0, \ldots, b_{i-1}]$. By Lemma 2.4.3, $A[b_0, \ldots, b_{n-1}, x]$ is a finitely generated A-module. Thus, by Proposition 2.4.2, x is integral over A. $\square$

Definition 2.4.5 (Integral closure, integrally closed)**.** If A is a subring of R, then the *integral closure of A in R* is the set A_c of elements of R that are integral ove rA. We say A is *integrally closed* in R if $A_c = A$.

Lemma 2.4.6. *If A is a subring of R, then A_c is a subring of R containing A.*

Proof. Clearly $A \subseteq A_c$, since $a \in A$ is a root of $X - a$. Suppose $x, y \in A_c$. As in the proof of Proposition 2.4.4, it follows from Lemma 2.4.3 that $A[x, y]$ is a finitely generated A-module. Since $x + y, x - y, xy \in A[x, y]$, these elements are all integral over by Proposition 2.4.2. $\square$

Lemma 2.4.7. *If A is a subring of the integral domain B, with B integral over A, then A is a field if and only if B is a field.*

Proof. The proof of this lemma is left as Exercises 2.4.2 and 2.4.3. $\square$

If $k \subseteq K$ are fields, we say that K is a *field extension* of k. This extension is said to be *finite* if K is finite dimensional as a k-vector space. For example $\mathbb{C}$ is a finite extension of $\mathbb{R}$, whereas $\mathbb{R}$ is *not* a finite extension of $\mathbb{Q}$.

Suppose K is a field extension of k. An element $a \in K$ is said to be *algebraic* over k if $f(a) = 0$ for some $f \in k[X]$. We say K is an *algebraic extension* of k if every element of K is algebraic over k. Note that since we are working over fields, the terms *integral* and *algebraic* become equivalent. (We can always divide by the leading coefficient of a polynomial to make it monic.)

Lemma 2.4.8. *Every finite extension of fields is an algebraic extension.*

Proof. Suppose K is a finite field extension of the field k. Let $a \in K$. Since K is finite dimensional over k, the infinite list of elements $1, a, a^2, a^3, \ldots$ cannot be linearly independent over k. Thus, there exists some $n \in \mathbb{Z}_{>0}$ and $c_0, \ldots, c_n \in k$ such that

$$c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0.$$

Hence a is algebraic over k. □

A field k is *algebraically closed* if every nonconstant polynomial $f \in k[X]$ has a root in k. Equivalently, k is algebraically closed if every nonconstant polynomial $f \in k[X]$ is a product of degree one polynomials. (See Exercise 2.4.4.)

Lemma 2.4.9. *If k is algebraically closed and K is a finite field extension of k, then $K = k$.*

Proof. Suppose k is algebraically closed and K is a finite field extension of k. Let $a \in K$. By Lemma 2.4.8, K is an algebraic extension of k, and so $f(a) = 0$ for some $f \in k[X]$. But since k is algebraically closed, we can factor f as

$$f = (X - a_1)(X - a_2) \cdots (X - a_n), \quad a_1, \ldots, a_n \in k.$$

It follows that $a = a_i$ for some $1 \leq i \leq n$. In particular, $a \in k$. □

Exercises.

2.4.1. Suppose S is a subring of a commutative ring R and the elements $x_1, \ldots, x_n \in R$ are algebraically independent over S. Show that $S[x_1, \ldots, x_n]$ is isomorphic as a ring to the polynomial ring $S[X_1, \ldots, X_n]$.

2.4.2 ([Ash, 7.1.3]). Suppose A is a subring of a field B, with B integral over A. Let a be a nonzero element of A. Then since $a^{-1} \in B$, there is an equation of the form

$$\left(a^{-1}\right)^n + c_{n-1}\left(a^{-1}\right)^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0,$$

with $c_i \in A$. Show that $a^{-1} \in A$, proving that A is a field.

2.4.3 ([Ash, 7.1.4, 7.1.5]). Suppose that a field A is a subring of the integral domain B, with B integral over A. Let b be a nonzero element of B. By Proposition 2.4.2, $A[b]$ is a finite-dimensional vector space over A. Let f be the A-linear transformation on this vector space given by multiplication by b. In other words, $f(z) = bz$, $z \in A[b]$. Show that f is bijective. Conclude that B is a field.

2.4.4. Prove that a field k is algebraically closed if and only if every nonconstant polynomial $f \in k[X]$ is a product of degree one polynomials.

2.5 Nother normalization lemma

Suppose R is a commutative ring. An (associative) R-algebra is an additive abelian group A that has the structure of both a ring and an R-module, and such that

$$r(ab) = (ra)b = a(rb), \quad a, b \in A, r \in R.$$

Equivalently, A is an R-module together with an R-bilinear map (multiplication)

$$A \times A \to A, \quad (a, b) \mapsto ab,$$

such that this multiplication is associative and has a multiplicative identity.

Examples 2.5.1. (a) A $\mathbb{Z}$-algebra is simply a ring. Precisely, if A is a ring we define the $\mathbb{Z}$-module structure by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ factors}} & n > 0, \\ 0 & n = 0, \\ \underbrace{-a - a - \cdots - a}_{-n \text{ factors}} & n < 0. \end{cases}$$

(b) The set $M_n(R)$ of $n \times n$ matrices with entries in the field R is an R-algebra with usual addition and multiplication of matrices.

(c) The polynomial ring $R[X_1, \ldots, X_n]$ is an R-algebra.

An R-algebra A is *finitely generated* if there are finitely many elements $x_1, \ldots, x_n \in A$ such that every element of A can be written as a polynomial in the x_i with coefficients in R, i.e. $A = R[x_1, \ldots, x_n]$. (We say that A is *generated as an R-algebra* by the x_i.) Equivalently, A is finitely generated if it is a homomorphic image of the polynomial algebra $R[X_1, \ldots, X_n]$ (see Exercise 2.2.2).

Suppose A is an R-algebra and $y_1, \ldots, y_r \in A$. The elements $y_1, \ldots, y_r \in A$ are *algebraically dependent* (over R) if there exists a nonzero $f \in R[X_1, \ldots, X_r]$ such that $f(y_1, \ldots, y_r) = 0$. Otherwise, the elements are said to be *algebraically independent*.

Proposition 2.5.2 (Noether normalization lemma)**.** *If A is a finitely generated k-algebra, then there exists a finite subset $\{y_1, \ldots, y_r\}$ of A such that the $y_1, \ldots, y_r$ are algebraically independent and A is integral over $k[y_1, \ldots, y_r]$.*

Proof. We will give the proof in the case that the field k is infinite. For the case where the field is finite, we refer the reader to [Ash, §8.3.8].

Choose a finite generating set $\{x_1, \ldots, x_n\}$ for A (as an algebra). Let $\{x_1, \ldots, x_r\}$ be a maximal algebraically independent subset of $\{x_1, \ldots, x_n\}$. If $n = r$, then we are finished, since we can take $y_i = x_i$ for all i. So we assume $r < n$. Thus $x_1, \ldots, x_n$ are algebraically dependent, and so there is a nonzero polynomial $f \in f[X_1, \ldots, X_n]$ such that $f(x_1, \ldots, x_n) = 0$.

We will prove the result by induction on n. If $n = 1$, then $r = 0$, in which case $A = k[x_1]$ and we can take $\{y_1, \ldots, y_r\}$ to be the empty set.

Now suppose $n > 1$ and that the result holds for $n-1$. Since f is nonzero and $f(x_1,\dots,x_n) = 0$, f is a nonconstant polynomial. Let d be the degree of f, and let g be the homogeneous component of degree d (i.e. g is the sum of all the degree d terms of f). So

$$f = g + \text{terms of degree less than } d.$$

Since g is homogeneous of degree d, we can write

$$g = g_0 X_n^d + g_1 X_n^{d-1} + \cdots + g_d,$$

where $g_i \in k[X_1,\dots,X_{n-1}]$ is homogeneous of degree i (or $g_i = 0$) for $0 \le i \le d$. Then

$$g(X_1,\dots,X_{n-1},1) = g_0 + \cdots + g_d \neq 0.$$

(Here we use the fact that at least one of the g_i is nonzero, since $g \neq 0$, and the fact that the nonzero g_i are all homogeneous of different degrees.) Since k is infinite, it follows from Proposition 2.1.5(b) that

$$g(a_1,\dots,a_{n-1},1) \neq 0 \quad \text{for some } a_1,\dots,a_{n-1} \in k.$$

For $i = 1,\dots,n-1$, let $z_i = x_i - a_i x_n$. Then we have

$$\begin{aligned} 0 &= f(x_1,\dots,x_n) \\ &= f(z_1 + a_1 x_n,\dots,z_n + a_n x_n) \\ &= g(a_1,\dots,a_{n-1},1)x_n^d + \text{ terms of degree less than } d \text{ in } x_n. \end{aligned}$$

Dividing by $g(a_1,\dots,a_n,1)$, we see that x_n is integral over $B = k[z_1,\dots,z_{n-1}]$. By the induction hypothesis, there are algebraically independent elements $y_1,\dots,y_r$ such that B is integral over $k[y_1,\dots,y_r]$. By Proposition 2.4.4, $x_1,\dots,x_n$ are integral over $k[y_1,\dots,y_r]$. Since A is generated by $x_1,\dots,x_n$, it follows from Lemma 2.4.6 that A is integral over $k[y_1,\dots,y_r]$. □

Recall that if I is an ideal of a ring R, then R/I is a field if and only if I is maximal (proper) ideal.

Corollary 2.5.3. *Let B be a finitely generated k-algebra. If I is a maximal ideal of B, then B/I is a finite extension of k.*

Proof. Consider the map

$$k \to B/I, \quad c \mapsto c + I,\ c \in k.$$

This map is injective, since if $c \in I$, then c must zero since $c \neq 0$ would imply that $1 = c^{-1}c \in I$, contradicting the fact that I is a proper ideal. Via this map, we view k as a subfield of B/I.

Since B is finitely generated k-algebra, so is $A := B/I$. Thus, it follows from Proposition 2.5.2 that there is a subset $\{y_1,\dots,y_r\}$ of A, algebraically independent over A, such that A is integral over $k[y_1,\dots,y_r]$. Since A is a field (because I is a maximal ideal), so is $k[y_1,\dots,y_r]$, by Lemma 2.4.7. Now, if $r \ge 1$, then the field $k[y_1,\dots,y_r]$ must contain y_1^{-1}, which implies that $y_1^{-1} = g(y_1,\dots,y_r) \in k[y_1,\dots,y_r]$. This gives $y_1 g(y_1,\dots,y_r) = 1$, contradicting the fact that the $y_1,\dots,y_r$ are algebraically independent.

Hence $r = 0$. Thus A is integral over the field k. Since A is also finitely generated over k, it follows that A is a finite extension of k (see Exercise 2.5.1). □

Corollary 2.5.4. *Let A be a finitely generated k-algebra, where k is a field. If A is itself a field, then A is a finite extension of k.*

Proof. If A is a field, then $I = \{0\}$ is a maximal ideal. Then the result follows from Corollary 2.5.3. □

Exercises.

2.5.1. Suppose A is a field extension of the field k that is finitely generated (as a k-algebra) and integral over k. Prove that A is a finite extension. *Hint*: Let $x_1, \ldots, x_n$ generate A. Then $x_1, \ldots, x_n$ are integral over k and $A = k[x_1, \ldots, x_n]$.

2.6 Hilbert Nullstellensatz

2.6.1 Statement of the theorem

The goal of this section is to prove the following result. We will break its proof into pieces.

Theorem 2.6.1. *For any field k and positive integer n, the following statements are equivalent.*

(a) The maximal ideals of $k[X_1, \ldots, X_n]$ are precisely the ideals of the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$, $a_1, \ldots, a_n \in k$. Thus, maximal ideals correspond to points.

(b) **Weak Nullstellensatz***: If I is an ideal of $k[X_1, \ldots, X_n]$ and $V(I) = \varnothing$, then $I = k[X_1, \ldots, X_n]$. Equivalently, if I is a proper ideal, then $V(I)$ is nonempty.*

(c) **Nullstellensatz***: If $I \trianglelefteq k[X_1, \ldots, X_n]$, then $IV(I) = \sqrt{I}$.*

(d) The field k is algebraically closed.

Before proving this theorem, let's give a couple examples.

Example 2.6.2. Consider the case $n = 1$. Since $k[X]$ is a principal ideal domain, all ideals of $k[X]$ are of the form $\langle f \rangle$ for some $f \in k[X]$. The ideal f is proper if and only if f is not a unit (i.e. it is not a nonzero constant polynomial). Then Theorem 2.6.1 says that

$$\begin{aligned} k \text{ is algebraically closed} &\iff V(I) \neq \varnothing \text{ for every proper ideal I} \\ &\iff V(f) \neq \varnothing \text{ for every nonconstant polynomial } f \in k[X] \\ &\iff \text{every nonconstant polynomial has a root.} \end{aligned}$$

Example 2.6.3. If $k = \mathbb{R}$, which is not algebraically closed, then we should be able to find proper ideals I such that $V(I) = \varnothing$. Indeed, $I = \langle x^2 + 1 \rangle$ is such an ideal.

2.6.2 The weak Nullstellensatz implies the Nullstellensatz

In this subsection, we will prove part of Theorem 2.6.1. Namely, we will prove that the weak Nullstellensatz implies the Nullstellensatz. So we suppose in this section that the weak Nullstellensatz holds.

Fix an ideal $I \trianglelefteq k[X_1, \dots, X_n]$. By Lemma 2.3.3, we have $\sqrt{I} \subseteq IV(I)$. Hence, it remains to prove the reverse inclusion.

Suppose $f \in IV(I)$. By the Hilbert Basis Theorem (Theorem 2.2.1), the ring $k[X_1, \dots, X_n]$ is noetherian, and so the ideal I is finitely generated. Choose generators $f_1, \dots, f_m$. Then define the ideal

$$I^* = \langle f_1, \dots, f_m, 1 - Yf \rangle \trianglelefteq k[X_1, \dots, X_n, Y].$$

Here we are viewing $f_1, \dots, f_m$ as elements of $k[X_1, \dots, X_n, Y]$ via the natural inclusion of $k[X_1, \dots, X_n]$ in $k[X_1, \dots, X_n, Y]$.

Lemma 2.6.4. *We have $V(I^*) = \varnothing$.*

Proof. Let $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{A}^{n+1}$. We split the proof into two cases.

Case 1: Suppose $(a_1, \dots, a_n) \in V(I)$. Then, since $f \in IV(I)$, we have $f(a_1, \dots, a_n) = 0$. Thus

$$(1 - Yf)(a_1, \dots, a_n, a_{n+1}) = 1 - a_{n+1} f(a_1, \dots, a_n) = 1 - a_{n+1} \cdot 0 = 1 \neq 0.$$

Since $1 - Yf \in I^*$, this implies that $(a_1, \dots, a_n, a_{n+1}) \notin V(I^*)$.

Case 2: Suppose $(a_1, \dots, a_n) \notin V(I)$. Then, for some $i \in \{1, \dots, m\}$, we have

$$f_i(a_1, \dots, a_n, a_{n+1}) = f_i(a_1, \dots, a_n) \neq 0.$$

Since $f_i \in I^*$, this implies that $(a_1, \dots, a_{n+1}) \notin V(I^*)$. □

Lemma 2.6.5. *There exist $g_1, \dots, g_m, h \in k[X_1, \dots, X_n, Y]$ such that*

$$1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf). \tag{2.4}$$

This equation also holds in the rational function field $k(X_1, \dots, X_n, Y)$ consisting of quotients of polynomials in $k[X_1, \dots, X_n, Y]$.

Proof. By Lemma 2.6.4, $V(I^*) = \varnothing$. Thus, by the weak Nullstellensatz, we have $I^* = k[X_1, \dots, X_n, Y]$. In particular, $1 \in I^*$. Since I^* is generated by $f_1, \dots, f_m, 1 - Yf$, we have an equation of the form (2.4). Since every polynomial is a rational function, this equation also holds in the rational function field. □

Lemma 2.6.6. *We have $f^r \in I$ for some positive integer r. Hence $f \in \sqrt{I}$.*

Proof. If $f = 0$, then $f \in I$ and we are done. Thus we suppose $f \neq 0$. Then consider the ring homomorphism

$$k[X_1, \dots, X_n, Y] \to k(X_1, \dots, X_n), \quad X_i \mapsto X_i,\ i = 1, \dots, n,\ Y \mapsto \frac{1}{f(X_1, \dots, X_n)}.$$

Applying this mapping to (2.4) gives

$$1 = \sum_{i=1}^{m} g\big(X_1, \ldots, X_n, 1/f(X_1, \ldots, X_n)\big) f_i(X_1, \ldots, X_n). \tag{2.5}$$

The right side of (2.5) is a sum of rational functions whose denominators are powers of f. Let f^r be the highest power that appears in these denominators. Multiplying both sides of (2.5) by f^r then yields an equation of the form

$$f^r = \sum_{i=1}^{m} h_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n),$$

where the h_i are *polynomials* in $k[X_1, \ldots, X_n]$. Hence $f^r \in I$. □

Corollary 2.6.7. *The weak Nullstellensatz implies the Nullstellensatz.*

Proof. We have shown above that, if we assume the weak Nullstellensatz, then $f \in \sqrt{I}$ for all $f \in IV(I)$. Combined with Lemma 2.3.3, this gives the Nullstellensatz. □

2.6.3 Proof of Theorem 2.6.1

(a) $\Longrightarrow$ (b): Suppose I is a proper ideal of $k[X_1, \ldots, X_n]$. We can choose a maximal ideal J containing I and, by Proposition 2.1.4(b), $V(J) \subseteq V(I)$. So it suffices to prove that $V(J) \neq \emptyset$. By (a), J has the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$. But then we clearly have $(a_1, \ldots, a_n) \in V(J)$. (In fact, we have $V(J) = \{a\}$.)

(b) $\Longrightarrow$ (c): This is Corollary 2.6.7.

(c) $\Longrightarrow$ (d): Suppose I is a proper ideal of $k[X_1, \ldots, X_n]$. Then I is contained in a maximal, hence prime, ideal P By Exercise 2.3.6, $\sqrt{I}$ is the intersection of all the prime ideals containing I. Hence $\sqrt{I} \subseteq P$. So $\sqrt{I}$ is a proper ideal. Thus, by (c), $IV(I)$ is a proper ideal. But $V(I) = \varnothing$, then $IV(I) = k[X_1, \ldots, X_n]$ by Proposition 2.1.5(a), which is a contradiction. So $V(I) \neq \varnothing$.

(d) $\Longrightarrow$ (a): Let I be a maximal ideal of $k[X_1, \ldots, X_n]$, and let $K = k[X_1, \ldots, X_n]/I$, which is a field containing an isomorphic copy of k via the map $c \mapsto c + I$, $c \in k$. Since K is a finitely generated k-algebra, it is a finite extension of k by Corollary 2.5.4. But then, since k is algebraically closed, we have $K = k$ by Lemma 2.4.9. Thus, for each $i = 1, \ldots, n$, we have

$$X_i + I = a_i + I \quad \text{for some } a_i \in k.$$

This implies that $X_i - a_i \in I$ for each $i = 1, \ldots, n$. So $\langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq I$. Since $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ is a maximal ideal by Lemma 2.3.1, we must have $I = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

(a) $\Longrightarrow$ (d): Let f be a nonconstant polynomial in $k[X_1]$. Then we can view f as a nonconstant polynomial in $k[X_1, \ldots, X_n]$. Let I be a maximal ideal containing the proper ideal $\langle r \rangle$. By (a), this is of the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$ for some $a = (a_1, \ldots, a_n \in \mathbb{A}^n$. Thus f vanishes at a, which means that $f(a_1) = 0$. Hence every nonconstant polynomial in $k[X_1]$ has a root. So k is algebraically closed.

Corollary 2.6.8. *Suppose $I, J \trianglelefteq k[X_1, \ldots, X_n]$, with k algebraically closed. If $V(I) = V(J)$ and $g \in I$, then $g^r \in J$ for some $r \in \mathbb{Z}_{>0}$.*

Proof. Suppose $V(I) = V(J)$ and $g \in I$. By Theorem 2.6.1, we have $\sqrt{I} = \sqrt{J}$. Thus $g \in I \subseteq \sqrt{I} = \sqrt{J}$, and so $g^r \in J$ for some $r \in \mathbb{Z}_{>0}$. □

Corollary 2.6.9. *Suppose k is an algebraically closed field. The maps*

$$V \mapsto I(V) \quad \text{and} \quad I \mapsto V(I)$$

give a one-to-one correspondence between varieties in $\mathbb{A}^n$ and radical ideals of $k[X_1, \ldots, X_n]$.

Proof. By Proposition 2.1.4(d), we have $VI(V)$ for any variety V. By Theorem 2.6.1, we have $VI(I) = \sqrt{I} = I$ for any radical ideal I. It remains to prove that $I(V)$ is a radical ideal for any variety V. Indeed, if $f^r \in I(V)$, then f^r vanishes on V. Thus f also vanishes on V, and so $f \in I(V)$. □

Corollary 2.6.10. *Suppose k is an algebraically closed field. Suppose $f_1, \ldots, f_r, g \in k[X_1, \ldots, X_n]$, and assume that g vanishes wherever the f_i all vanish. Then*

$$g^s = h_1 f_1 + \ldots + h_r f_r \quad \text{for some } s \in \mathbb{Z}_{>0},\ h_1, \ldots, h_r \in k[X_1, \ldots, X_n].$$

Proof. Let $I = \langle f_1, \ldots, f_r \rangle$. By assumption $g \in IV(I) = \sqrt{I}$ (using Theorem 2.6.1). Thus $g^s \in I$ for some $s \in \mathbb{Z}_{>0}$, and the result follows. □

Exercises.

Recall that $f \in k[X_1, \ldots, X_n]$ is *irreducible* if $f \neq 0$ and whenever $f = gh$, we have that either g or h is a unit (i.e. invertible element) in $k[X_1, \ldots, X_n]$. In addition, f is irreducible if and only if $\langle f \rangle$ is a nonzero prime ideal. Since $k[X_1, \ldots, X_n]$ is a unique factorization domain, every element factors as a product of irreducibles. This factorization is unique up to reordering and multiplication by units.

2.6.1 ([Ash, Prob. 8.3.3]). An *algebraic curve* is a variety of the form $V(f)$ for $f \in k[X, Y]$, with f nonconstant. Show that, if k is algebraically closed, then two nonconstant polynomials $f, g \in k[X, Y]$ define the same algebraic curve if and only if f divides some power of g and g divides some power of f (equivalently, f and g have the same irreducible factors).

2.6.2 ([Ash, Prob. 8.4.1, 8.4.2]). Let $f \in k[X_1, \ldots, X_n]$ and assume that the factorization of f into irreducibles is $f = f_1^{n_1} \cdots f_r^{n_r}$.

(a) Show that the decomposition of the variety $V(f)$ into irreducible subvarieties (see Exercise 2.1.7) is given by $V(f) = \bigcup_{i=1}^{r} V(f_i)$.

(b) Show that $IV(f) = (f_1 \cdots f_r)$.

2.6.3 ([Ash, Prob. 8.4.3]). Show that there is a one-to-one correspondence between irreducible polynomials in $k[X_1, \ldots, X_n]$ and irreducible hypersurfaces, if polynomials that differ by a nonzero multiplicative constant are identified.

2.6.4 ([Ash, Prob. 8.4.4]). For any collection of subsets X_i of $\mathbb{A}^n$, show that $I(\bigcup_i X_i) = \bigcap_i I(X_i)$.

2.6.5 ([Ash, Prob. 8.4.5, 8.4.6]). (a) Show that every radical ideal I of $k[X_1, \ldots, X_n]$ is the intersection of finitely many prime ideals.

(b) Show that this decomposition is unique, subject to the condition that the prime ideals P are *minimal*, that is, there is no prime ideal Q such that $I \subseteq Q \subsetneq P$.

2.6.6 ([Ash, Prob. 8.4.7]). Suppose that X is a variety in $\mathbb{A}^2$, defined by equations

$$f_1(x, y) = f_2(x, y) = \cdots = f_m(x, y) = 0, \quad m \geq 2.$$

Let g be the greatest common divisor of the f_i. If g is constant, show that X is a finite set (possibly empty).

2.6.7 ([Ash, Prob. 8.4.8]). Show that every variety in $\mathbb{A}^2$ except for $\mathbb{A}^2$ itself is the union of a finite set and an algebraic curve.

2.6.8 ([Ash, Prob. 8.4.9]). Give an example of two distinct irreducible polynomials in $k[X, Y]$ with the same zero-set, and explain why this cannot happen if k is algebraically closed.

2.6.9. Suppose B is a k-algebra, with k an algebraically closed field. Show that B is isomorphic to the coordinate ring of some variety if and only if B is a finitely generated k-algebra with no nonzero nilpotent elements (see Exercise 2.3.4).

Index

Bibliography

[Ash] R. Ash. *Abstract algebra: The Basic Graduate Year*. URL: https://faculty.math.illinois.edu/~r-ash/Algebra.html.

[Jud] T. W. Judson. *Abstract algebra: theory and applications*. URL: http://abstract.ups.edu/.

[Sav] A. Savage. Ring theory. Notes for MAT 3141. URL: http://alistairsavage.ca/mat3143/notes/MAT3143-Ring_theory.pdf.