Introduction to Commutative Algebra

M. F. ATIYAH I. G. MACDONALD

October 29, 2022

Contents

Introduction

Commutative algebra is essentially the study of commutative rings. Roughly speaking, it has developed from two sources: (1) algebraic geometry and (2) algebraic number theory. In (1) the prototype of the rings studied is the ring $k[x_1, \cdots, x_n]$ of polynomials in several variables over a field k; in (2) it is the ring $\mathbf{Z}$ of rational integers. Of these two the algebro-geometric case is the more far-reaching and, in its modern development by Grothendieck, it embraces much of algebraic number theory. Commutative algebra is now one of the foundation stones of this new algebraic geometry. It provides the complete local tools for the subject in much the same way as differential analysis provides the tools for differential geometry.

This book grew out of a course of lectures given to third year under- graduates at Oxford University and it has the modest aim of providing a rapid introduction to the subject. It is designed to be read by students who have had a first elementary course in general algebra. On the other hand, it is not intended as a substitute for the more voluminous tracts on commutative algebra such as Zariski-Samuel [4] or Bourbaki [1]. We have concentrated on certain central topics, and large areas, such as field theory, are not touched. In content we cover rather more ground than Northcott [3] and our treatment is substantially different in that, following the modern trend, we put more emphasis on modules and localization.

The central notion in commutative algebra is that of a prime ideal. This provides a common generalization of the primes of arithmetic and the points of geometry. The geometric notion of concentrating attention "near a point" has as its algebraic analogue the important process of localizing a ring at a prime ideal. It is not surprising, therefore, that results about localization can usefully be thought of in geometric terms. This is done methodically in Grothendieck's theory of schemes and, partly as an introduction to Grothendieck's work [2], and partly because of the geometric insight it provides, we have added schematic versions of many results in the form of exercises and remarks.

The lecture-note origin of this book accounts for the rather terse style with little general padding, and for the condensed account of many proofs. We have resisted the temptation to expand it in the hope that the brevity of our presentation will make clearer the mathematical structure of what is by now an elegant and attractive theory. Our philosophy has been to build up to the main theorems in a succession of simple steps and to omit routine verifications.

Anyone writing now on commutative algebra faces a dilemma in connection with homological algebra, which plays such an important part in modern developments. A proper treatment of homological algebra is impossible within the confines of a small book: on the other hand, it is hardly sensible to ignore it completely. The compromise we have adopted is to use elementary homological methods-exact sequences, diagrams, etc.-but to stop short of any results requiring a deep study of homology. In this way we hope to prepare the ground for a systematic course on homological algebra which the reader should undertake if he wishes to pursue algebraic geometry in any depth.

We have provided a substantial number of exercises at the end of each chapter. Some of them are easy and some of them are hard. Usually we have provided hints, and sometimes complete solutions, to the hard ones. We are indebted to Mr. R. Y. Sharp, who worked through them all and saved us from error more than once.

We have made no attempt to describe the contributions of the many mathematicians who have helped to develop the theory as expounded in this book. We would, however, like to put on record our indebtedness to J.-P. Serre and J. Tate from whom we learnt the subject, and whose influence was the determining factor in our choice of material and mode of presentation.

References

[1] N Bourbaki. "Algèbre commutative, Hermann". In: *Paris, 1961–65* (1961).

[2] A Grothendieck and J Dieudonné. "Éléments de Géométrie algébrique". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 4.1 (1960), pp. 5–214.

[3] D. G. Northcott. *Ideal Theory*. Cambridge University Press, 1953.

[4] Oscar Zariski and Pierre Samuel. *Commutative algebra I, II*. Vol. 1. 1958, 1960.

Notation and Terminology

Rings and modules are denoted by capital italic letters, elements of them by small italic letters. A field is often denoted by k. Ideals are denoted by small German characters. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ denote respectively the ring of rational integers, the field of rational numbers, the field of real numbers and the field of complex numbers.

Mappings are consistently written on the *left*, thus the image of an element x under a mapping f is written $f(x)$ and not $(x)f$. The composition of mappings $f : X \to Y, g : Y \to Z$ is therefore $g \circ f$, not $f \circ g$. A mapping $f : X \to Y$is *injective* if $f(x_1) = f(x_2)$ implies $x_1 = x_2$; surjective if $f(X) = Y$; bijective if both injective and surjective.

The end of a proof (or absence of proof) is marked thus $\square$.

Inclusion of sets is denoted by the sign $\subseteq$. We reserve the sign $\subset$ for strict inclusion. Thus $A \subset B$ means that A is contained in B and is not equal to B.

Chapter 1

Rings and Ideals

Chapter 2

Modules

Chapter 3

Rings and Modules of Fractions

Chapter 4

Primary Decomposition

The decomposition of an ideal into primary ideals is a traditional pillar of ideal theory. It provides the algebraic foundation for decomposing an algebraic variety into its irreducible components—although it is only fair to point out that the algebraic picture is more complicated than naïve geometry would suggest. From another point of view primary decomposition provides a generalization of the factorization of an integer as a product of prime-powers. In the modern treatment, with its emphasis on localization, primary decomposition is no longer such a central tool in the theory. It is still, however, of interest in itself and in this chapter we establish the classical uniqueness theorems.

The prototypes of commutative rings are $\mathbf{Z}$ and the ring of polynomials $k[x_1, \cdots, x_n]$ where k is a field; both these are unique factorization domains. This is not true of arbitrary commutative rings, even if they are integral domains (the classical example is the ring $\mathbf{Z}[\sqrt{-5}]$, in which the element 6 has two essentially distinct factorizations, $2 \cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$. However, there is a generalized form of "unique factorization" of *ideals* (not of elements) in a wide class of rings (the Noetherian rings).

A prime ideal in a ring A is in some sense a generalization of a prime number. The corresponding generalization of a power of a prime number is a primary ideal. An ideal $\mathfrak{q}$ in a ring A is *primary* if $\mathfrak{q} \neq A$ and if

$$xy \in \mathfrak{q} \implies \text{either } x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0.$$

In other words,

$$\mathfrak{q} \text{ is primary} \iff A/\mathfrak{q} \neq 0 \text{ and every zero-divisor in } A/\mathfrak{q} \text{ is nilpotent.}$$

Clearly every prime ideal is primary. Also the contraction of a primary ideal is primary, for if $f : A \to B$ and if $\mathfrak{q}$ is a primary ideal in B , then $A/\mathfrak{q}^c$ is isomorphic to a subring of $B/\mathfrak{q}$.

Proposition 4.1. *Let $\mathfrak{q}$ be a primary ideal in a ring A. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. By (1.8) it is enough to show that $\mathfrak{p} = r(\mathfrak{q})$ is prime. Let $xy \in r(\mathfrak{q})$, then $(xy)^m \in \mathfrak{q}$ for some $m > 0$, and therefore either $x^m \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$ for some $n > 0$; i.e., either $x \in r(\mathfrak{q})$ or $y \in r(\mathfrak{q})$. □

If $\mathfrak{p} = r(\mathfrak{q})$, then $\mathfrak{q}$ is said to be $\mathfrak{p}$-primary.

Example. *1. The primary ideals in* $\mathbf{Z}$ *are* (0) *and* (p^n)*, where* p *is prime. For these are the only ideals in* $\mathbf{Z}$ *with prime radical, and it is immediately checked that they are primary.*

2. Let $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$*. Then* $A/\mathfrak{q} \simeq k[y]/(y^2)$*, in which the zero-divisors are all the multiples of* y*, hence are nilpotent. Hence* $\mathfrak{q}$ *is primary, and its radical* $\mathfrak{p}$ *is* (x, y)*. We have* $\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}$ *(strict inclusions), so that a primary ideal is not necessarily a prime-power.*

3. Conversely, a prime power $\mathfrak{p}^n$ *is not necessarily primary, although its radical is the prime ideal* $\mathfrak{p}$*. For example, let* $A = k[x, y, z]/(xy - z^2)$ *and let* $\bar{x}, \bar{y}, \bar{z}$ *denote the images of* x, y, z *respectively in* A*. Then* $\mathfrak{p} = (\bar{x}, \bar{z})$ *is prime (since* $A/\mathfrak{p} \simeq k[y]$*, an integral domain); we have* $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ *but* $x \notin \mathfrak{p}^2$ *and* $y \notin r(\mathfrak{p}^2) = \mathfrak{p}$*; hence* $\mathfrak{p}^2$ *is not primary. However, there is the following result:*

Proposition 4.2. *If* $r(\mathfrak{a})$ *is maximal, then* $\mathfrak{a}$ *is primary. In particular, the powers of a maximal ideal* $\mathfrak{m}$ *are* $\mathfrak{m}$*-primary.*

Proof. Let $r(\mathfrak{a}) = \mathfrak{m}$. The image of $\mathfrak{m}$ in $A/\mathfrak{a}$ is the nilradical of $A/\mathfrak{a}$, hence $A/\mathfrak{a}$ has only one prime ideal, by (1.8). Hence every element of $A/\mathfrak{a}$ is either a unit or nilpotent, and so every zero-divisor in $A/\mathfrak{a}$ is nilpotent. □

We are going to study presentations of an ideal as an intersection of primary ideals. First, a couple of lemmas:

lemma 4.3. *If* $\mathfrak{q}_i$*,* $(1 \leq i \leq n)$ *are* $\mathfrak{p}$*-primary, then* $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ *is* $\mathfrak{p}$*-primary.*

Proof. $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \cap r(\mathfrak{q}_i) = \mathfrak{p}$. Let $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$. Then for some i we have $xy \in \mathfrak{q}_i$ and $y \notin \mathfrak{q}_i$ hence $x \in \mathfrak{p}$. since $\mathfrak{q}_i$ is primary. □

lemma 4.4. *Let* q *be a* $\mathfrak{p}$*-primary ideal,* x *an element of* A*. Then*

1. if $x \in \mathfrak{q}$ *then* $(\mathfrak{q} : x) = (1)$*;*

2. if $x \notin \mathfrak{q}$ *then* $(\mathfrak{q} : x)$ *is* $\mathfrak{p}$*-primary, and therefore* $r(\mathfrak{q} : x) = \mathfrak{p}$*;*

3. if $x \notin \mathfrak{p}$ *then* $(\mathfrak{q} : x) = \mathfrak{q}$*.*

Proof. i) and iii) follow immediately from the definitions. ii): if $y \in (\mathfrak{q} : x)$ then $xy \in \mathfrak{q}$, hence (as $x \notin \mathfrak{q}$) we have $y \in \mathfrak{p}$ Hence $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$;taking radicals, we get $r(\mathfrak{q} : x) = \mathfrak{p}$. Let $yz \in (\mathfrak{q} : x)$ with $y \notin \mathfrak{p}$; then $xyz \in \mathfrak{q}$, hence $xz \in \mathfrak{q}$, hence $z \in (\mathfrak{q} : x)$. □

A primary decomposition of an ideal a in A is an expression of a as a finite intersection of primary ideals, say

$$a = \bigcap_{i=1}^{n} \mathfrak{q}_i \tag{4.1}$$

(In general such a primary decomposition need not exist; in this chapter we shall restrict our attention to ideals which have a primary decomposition.) If more