MA557: Commutative Algebra

Takumi Murayama

Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907-2067, USA
Email address: murayama@purdue.edu

2020 *Mathematics Subject Classification.* 13

This material is based upon work supported by the
National Science Foundation under Grant No. DMS-2201251.

Compiled September 22, 2025.

Contents

List of Symbols ix

Conventions xi

Preface xiii

Chapter 1. Rings and ideals 1
1.1. Rings and fields 1
1.2. When do polynomials generate a polynomial ring? 2
1.3. Ideals and quotient rings 4
1.4. Radical, prime, and maximal ideals 8
1.5. Zorn's lemma and applications to prime ideals 11
1.6. Spectra as topological spaces 13
1.7. Product rings and their spectra 16
1.8. Hartshorne's conjecture 17

Chapter 2. Modules 19
2.1. Categories 19
2.2. Definitions of modules 23
2.3. Quotient modules 26
2.4. Formal power series rings 28
2.5. Exact sequences 29

Chapter 3. Localization 31
3.1. Algebras 31
3.2. Localization of rings 32
3.3. Restriction of scalars 37
3.4. Localization of modules 37
3.5. Local properties 39
3.6. More on Spec 41

Chapter 4. Integral extensions 45
4.1. Motivation: How can we tell rings apart? 45
4.2. Integral extensions 46
4.3. Lying over and incomparability 52
4.4. Going up 54
4.5. Cardinality of fibers of module-finite maps 56
4.6. More on representable functors 58
4.7. Going down 60

Chapter 5. Noether's normalization theorem and Hilbert's Nullstellensatz 65

5.1. Algebraic sets 65
5.2. Noether's normalization theorem 65
5.3. Hilbert's Nullstellensatz 69
5.4. Effective Nullstellensatz (not covered in class) 72
5.5. Dimension theory for k-algebras 73
5.6. Valuation rings 76
5.7. Back to dimension theory 77

Chapter 6. Chain conditions 81
6.1. Chain conditions in general 81
6.2. Chain conditions for rings and modules 81
6.3. Hilbert's basis theorem 85
6.4. Noetherian induction 86
6.5. Examples of Artinian modules that are not Noetherian 86
6.6. More on algebraic sets 88
6.7. Noetherian topological spaces 89
6.8. The category of algebraic sets 92
6.9. Noether's theorem on rings of invariants 97
6.10. Hilbert's basis theorem for formal power series 98

Chapter 7. Tensor products and flatness 101
7.1. Definition of tensor products 101
7.2. Right exactness of tensor products and flatness 104
7.3. Tensor products of multiple factors 105
7.4. Extension of scalars 106
7.5. Presentations and extension of scalars 108
7.6. Tensor–Hom adjunction 109
7.7. Left exactness of Hom 110
7.8. Projective modules 112
7.9. A projective module that is not free 113
7.10. Projective modules over local rings 114
7.11. Tensor products of algebras 117
7.12. Examples 118
7.13. Colon ideals 121
7.14. More local properties 122

Chapter 8. Primary decomposition 125
8.1. Motivation 125
8.2. Primary ideals 125
8.3. Primary decompositions 126
8.4. Existence of primary decompositions 127
8.5. Uniqueness of primary decompositions 128
8.6. Associated primes 130
8.7. Prime cyclic filtrations and dévissage 132
8.8. Behavior under localization 133
8.9. Primary decomposition and associated primes 136
8.10. Krull's intersection theorem 137
8.11. Artinian rings are Noetherian 137
8.12. Krull's height theorem and systems of parameters 141

8.13. Dimension of formal power series rings 144
8.14. Dimension for modules 145
8.15. Regular sequences and depth 146
8.16. Cohen–Macaulay rings and modules 148
8.17. More on depth 151
8.18. Depth in short exact sequences 154

Chapter 9. Normal rings, DVRs, and Dedekind domains 157
9.1. Dedekind domains 157
9.2. Krull and Serre's criteria for normality 157
9.3. Primary decomposition and divisor class groups 160
9.4. More on normal domains 164
9.5. Noetherianity of integral closures 165
9.6. Classification of modules over a Dedekind domain (not covered in class) 169

Chapter 10. Completions 173
10.1. Motivation 173
10.2. Direct limits and inverse limits 173
10.3. Completions of rings and modules 177
10.4. The Artin–Rees lemma 182
10.5. Further applications of completions 187

Index 191

Bibliography 197

List of Symbols

Symbol	Description
$-x$	additive inverse of an element x, 1
0	zero element or zero ring, 1
1	identity element in a ring R, xi, 1
$\mathbf{C}$	complex numbers
$\mathbf{F}_q$	finite field with q elements, 2
$\mathbf{N}$	natural numbers $\{0, 1, 2, \ldots\}$
$\mathbf{Q}$	rational numbers
$\mathbf{R}$	real numbers
$\mathbf{Z}$	integers, 2
Ab	category of Abelian groups, 20
Grp	category of groups, 19
Rings	category of rings, 19
Sets	category of sets, 19
Top	category of topological spaces, 20
Vect_k	category of vector spaces over a field k, 21
$\mathfrak{C}_I(M)$	Cauchy sequences for the I-adic topology, 177
$\mathfrak{C}_I^0(M)$	null sequences for the I-adic topology, 178
$\mathfrak{m}_P$	ideal of a point in $\mathbf{A}_k^n$, 88
$A - B$	set difference, xi
$\mathrm{Ann}_R(M)$	annihilator of an R-module M, 25
$\mathrm{Ann}_R(m)$	annhilator of an element m in an R-module, 25
$\mathrm{Ass}_R(M)$	associated primes of M, 131
$\mathrm{Bil}_R(M, N; W)$	R-bilinear maps $M \times N \to W$, 101
$\mathrm{Cl}(R)$	the divisor class group of a normal Noetherian domain R, 161
$\mathcal{C}^{\mathrm{op}}$	opposite category, 19
$D(f)$	complement of $V(f)$, 14
$\deg(f)$	degree of a polynomial f, 2
$\mathrm{depth}_I(M)$	I-depth of a module M, 148
$\dim(M)$	Krull dimension of a module M, 145
$\dim(R)$	Krull dimension of a ring R, 45
$\mathrm{div}(a)$	the divisor of an element a in a normal Noetherian domain, 160
$\mathrm{End}_R(M)$	endomorphism ring of an R-module M, 47
$\mathrm{Fun}(\mathcal{C}, \mathcal{D})$	functors $\mathcal{C} \to \mathcal{D}$, 59
$\mathrm{ht}(P)$	height of a prime ideal P, 55
$I(X)$	ideal of a subset of $\mathbf{A}_k^n$, 88
$k[X]$	coordinate ring of an algebraic set $X \subseteq \mathbf{A}_k^n$, 93

Symbol	Description
$\ker(\varphi)$	kernel of a homomorphism φ, 5
$\varinjlim_i X_i$	direct limit of a direct system $\{X_i, f_{ij}\}$, 174
$\varprojlim_i X_i$	inverse limit of an inverse system $\{X_i, f_{ij}\}$, 177
$\ell_R(M)$	length of an R-module M, 138
$\operatorname{MaxSpec}(R)$	maximal spectrum of a ring R, 10
$\widehat{M}^I$	I-adic completion of a module M, 178
$M \otimes_R N$	tensor product of M and N over R, 102
$Q^{(n)}$	n-th symbolic power of a prime ideal Q, 141
$R[x]$	polynomial ring over a ring R, 2
R^G	invariant subring under the action of a group G, 97
$\operatorname{Spec}(R)$	spectrum of a ring R, 10
$\operatorname{Supp}(M)$	support of a module M, 39
$T(M)$	torsion submodule of an R-module M, 25
$T \star S$	composition of two natural transformations T and S, 21
$V(I)$	the set of prime ideals containing I, 13
V^*	dual of a vector space V, 21
$v_P(I)$	valuation of an ideal in a DVR, 163
$W^{-1}M$	localization of a module M at W, 38
$W^{-1}R$	localization of a ring R at W, 32
x^{-1}	multiplicative inverse of an element x, 2
$Z(I)$	algebraic set defined by an ideal I, 65

Conventions

(1) Let A and B be subsets of a set X. The *set difference* is denoted

$$A - B \coloneqq \big\{x \in X \,\big|\, x \in A \text{ and } x \notin B\big\}.$$

[AK21, (1.1)]

(2) All rings R will be assumed to be commutative with an identity element 1, unless stated otherwise. We will sometimes denote 1 by 1_R for clarity. [Rei95, (1.1)] [Hoc17, p. 1]

(3) All ring homomorphisms $\varphi\colon R \to S$ will be assumed to respect the identity element, i.e., $\varphi(1_R) = 1_S$. [AM69, pp. 1–2]

Preface

These are notes for a graduate course on commutative algebra (MA557) taught at Purdue University in Fall 2024. I taught a previous version of this course as an undergraduate course at Princeton University in Fall 2020. The official course text is [Hoc17], although the lectures also draw from [AM69; Rei95; AK21]. The notes in the margins point to where in these texts one can find the material written down in these notes. These notes will be continually updated throughout the semester.

I would like to thank Farrah Yhee for innumerable helpful conversations. I am also grateful to Margherita Barile, Winfried Bruns, Melvin Hochster, Gennady Lyubeznik, and Peter Schenzel for their thoughts about questions related to Open Problem 1.8.1.

CHAPTER 1

Rings and ideals

8/19

Commutative algebra is the study of commutative rings and of modules over commutative rings. The necessity to study these objects arose in two fields: [AM69, p. vii]

(1) algebraic geometry, where the fundamental objects are polynomial rings $k[x_1, x_2, \ldots, x_n]$ over a field k; and
(2) algebraic number theory, where the fundamental objects are the integers $\mathbf{Z}$ and rings of algebraic integers.

See, e.g., [BouCA, p. 579ff] and [Cor04] for some history of the subject.

1.1. Rings and fields

We recall the notion of a ring. In this form, this notion is essentially due to Emmy Noether [Noe1921, p. 29], although she did not assume the existence of an identity element in Definition 1.1.1(4). The word "ring" is due to Hilbert [Hil1897, §31]. See [Cor00] for more history.

DEFINITION 1.1.1. A *ring* R is a set with two binary operations, addition and multiplication, such that [AK21, (1.1)] [Rei95, (1.1)] [Hoc17, p. 1] [AM69, p. 1]

(1) R is an abelian group with respect to addition, in which case
   - R has a zero element 0; and
   - every $x \in R$ has an (additive) inverse $-x$.
(2) The multiplication on R satisfies
   - associativity: $(xy)z = x(yz)$ for all $x, y, z \in R$; and
   - distributivity over addition:
   $$x(y+z) = xy + xz \quad \text{and} \quad (y+z)x = yx + zx$$
   for all $x, y, z \in R$.

Unless otherwise specified, we will assume that R is *commutative*, i.e.,

(3) $xy = yx$ for all $x, y \in R$,

and that R has an *identity element*, i.e.,

(4) There exists an element $1 \in R$ (sometimes written 1_R for clarity) such that $x1 = 1x = x$ for all $x \in R$.[1]

REMARK 1.1.2. It can be the case that $1 = 0$ in Definition 1.1.1(4). In this case, R is the *zero ring*, which we denote by 0, since for every $x \in R$, we have

$$x = x1 = x0 = 0.$$

We also recall the following definition due to Weber [Web1893].

[1] See [Poo19] for reasons why rings should have an identity element. In short the existence of an identity element follows from a version of the associativity axiom where one of the groupings is allowed to have zero elements.

[AK21, (2.3)]
[AM69, pp. 1–2]

DEFINITION 1.1.3 [Web1893, pp. 526–527]. A *field* k is a ring such that $1 \neq 0$ and such that every nonzero element admits a multiplicative inverse, i.e., for every nonzero element $x \in k$, there exists an element denoted x^{-1} such that $xx^{-1} = 1$.

EXAMPLE 1.1.4. Here are some examples of rings.

(1) The integers $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots, \}$.
(2) The rational numbers $\mathbf{Q}$.
(3) The real numbers $\mathbf{R}$.
(4) The complex numbers $\mathbf{C}$.
(5) The finite field $\mathbf{F}_q$ with q elements, where q is a positive prime power.

The last four are all fields. In addition, if R is a ring, then the *polynomial ring* over R is the ring

$$R[x] \coloneqq \left\{ \sum_{i=0}^{d} r_i x^i \;\middle|\; r_i \in R,\ d < \infty \right\},$$

where addition is given by

$$\sum_i r_i x^i + \sum_i s_i x^i = \sum_i (r_i + s_i) x^i$$

and multiplication is given by

$$\left(\sum_i r_i x^i \right) \left(\sum_j s_j x^j \right) = \sum_n \left(\sum_{i+j=n} r_i s_j \right) x^n.$$

The *degree* $\deg(f)$ of a polynomial $f \in R[x]$ is the largest integer i such that $r_i \neq 0$.

We now define maps between rings.

[AK21, (1.1)]
[Rei95, (1.1)]
[Hoc17, p. 1]
[AM69, p. 2]

DEFINITION 1.1.5. Let R and S be rings. A *ring map* $\varphi\colon R \to S$ is a map such that for every $x, y \in R$, we have

(1) $\varphi(x + y) = \varphi(x) + \varphi(y)$, i.e., φ is a map of abelian groups, in which case
$$\varphi(x - y) = \varphi(x) - \varphi(y), \quad \varphi(-x) = -\varphi(x), \quad \varphi(0) = 0.$$
(2) $\varphi(xy) = \varphi(x)\,\varphi(y)$.

We will also assume that ring maps respect the identity element, i.e.,

(3) $\varphi(1_R) = 1_S$.

A ring map φ is an *isomorphism* if it is bijective.

A subset $R \subseteq S$ of a ring S is a *subring* of S if the inclusion $R \subseteq S$ is a ring map.

[Hoc17, pp. 2–4]

1.2. When do polynomials generate a polynomial ring?

To motivate this course, we give some examples of problems in commutative algebra, most of which are still open.

We first set some notation. Let R be a ring. If S is another ring, we will write

$$S = R[\theta_1, \theta_2, \dots, \theta_n]$$

to mean that S is *generated* by the elements $\theta_1, \theta_2, \dots, \theta_n$ as a ring over a subring $R \subseteq S$, i.e., the ring S contains R and the elements $\theta_1, \theta_2, \dots, \theta_n$, and there are no

strictly smaller subrings of S containing R. It also means that every element in S can be written (not necessarily uniquely) as a finite linear combination

$$\sum_{\nu \in \mathbf{N}^n} r_\nu \, \theta_1^{\nu_1} \theta_2^{\nu_2} \cdots \theta_n^{\nu_n},$$

where $r_\nu \in R$ for every $\nu \in \mathbf{N}^n$.

Our first guiding question is the following:

QUESTION 1.2.1. *Consider two complex polynomials $f, g \in \mathbf{C}[x]$. Can we tell whether f and g generate $\mathbf{C}[x]$? In other words, when is $\mathbf{C}[f, g] = \mathbf{C}[x]$?*

For example, we can consider the polynomials

$$f = x^5 + x^3 - x^2 + 1 \qquad \text{and} \qquad g = x^{14} - x^7 + x^2 + 5.$$

Then, since neither f nor g contain a term involving x with a nonzero coefficient, we see that they cannot generate all of $\mathbf{C}[x]$. On the other hand, if we just add the term x in f and consider

$$f = x^5 + x^3 - x^2 + x + 1 \qquad \text{and} \qquad g = x^{14} - x^7 + x^2 + 5, \tag{1.2.2}$$

then suddenly it is not so easy to answer Question 1.2.1. To tackle this sort of problem, we have the following theorem proved independently by Suzuki [Suz74] and by Abhyankar and Moh [AM75]:

THEOREM 1.2.3 [Suz74, Theorem 5; AM75, Main Theorem 4.2]. *Let $f, g \in \mathbf{C}[x]$ be complex polynomials of degree d and e, respectively. If $\mathbf{C}[f, g] = \mathbf{C}[x]$, then either $d \mid e$ or $e \mid d$, i.e., one of the two degrees must divide the other.*

Suzuki's proof uses complex analysis, while Abhyankar and Moh's proof uses what they call "high school algebra," yielding a version of Theorem 1.2.3 that holds over arbitrary fields. Since then, various proofs have appeared, including one using knot theory [Rud82].

The Abhyankar–Moh–Suzuki Theorem 1.2.3 gives an algorithm for deciding Question 1.2.1. For f and g as in (1.2.2), we see that Theorem 1.2.3 immediately tells us that $\mathbf{C}[f, g] \neq \mathbf{C}[x]$. On the other hand, if we replace x^{14} with x^{15} in (1.2.2) and consider

$$f = x^5 + x^3 - x^2 + x + 1 \quad \text{and} \quad g = x^{15} - x^7 + x^2 + 5, \tag{1.2.4}$$

we see that Theorem 1.2.3 does not tell us anything right away. Instead, we can cancel the leading terms in f and g and consider

$$\begin{aligned} g - f^3 = -3x^{13} + 3x^{12} - 6x^{11} + 3x^{10} - 10x^9 + 3x^8 - 4x^7 \\ - 2x^6 \ - 3x^5 \ - 6x^4 \ + 2x^3 \ + x^2 \ - 3x \ + 4 \end{aligned}$$

Note that f and $g - f^3$ generate the same subring in $\mathbf{C}[x]$ as f and g do. Moreover, the sum of the degrees of f and $g - f^3$ is strictly smaller than the sum of the degrees of f and g:

$$5 + 13 = 18 < 20 = 5 + 15.$$

Thus, we have reduced our problem to a "smaller" problem. Continuing in this manner, we will eventually be in one of three cases:

(1) The Abhyankar–Moh–Suzuki Theorem 1.2.3 applies, in the sense that neither $d \mid e$ nor $e \mid d$ (this is the case for (1.2.4), since $5 \nmid 13$ and $13 \nmid 5$);
(2) We get a constant and a single polynomial of degree ≥ 2; or

(3) One of the polynomials has degree 1.

In the first two cases, $\mathbf{C}[f,g] \neq \mathbf{C}[x]$, and in the last case, $\mathbf{C}[f,g] = \mathbf{C}[x]$. We note that this argument can actually be used for any pair of polynomials f and g, fully answering Question 1.2.1.

In two variables, however, the corresponding question is unsolved.

CONJECTURE 1.2.5 (Keller's Conjecture or the Jacobian Conjecture [Kel39]). *Consider two complex polynomials $f, g \in \mathbf{C}[x,y]$. Then, f and g generate $\mathbf{C}[x,y]$ if and only if the Jacobian determinant*

$$\det \begin{pmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y} \end{pmatrix}$$

is identically a nonzero constant.

See [vdE00] for an overview of what is known about the Jacobian Conjecture 1.2.5, where versions in a larger number of variables are also considered. We note that Conjecture 1.2.5 has a purely algebro-geometric statement in terms of polynomial endomorphisms of $\mathbf{C}^2$.

1.3. Ideals and quotient rings

Before moving on to other open questions, we define ideals and quotient rings. The following definition is also essentially due to Emmy Noether [Noe1921, p. 30]. See [Edw80] for more history.

[AK21, (1.4)] [Rei95, (1.2)] [AM69, p. 2]

DEFINITION 1.3.1. Let R be a ring. A subset $I \subseteq R$ is an *ideal* if it is an additive subgroup and if for every $x \in I$ and $y \in R$, we have $xy \in I$. An ideal is *proper* if $I \subsetneq R$, or equivalently if $1 \notin R$.

If $\{f_\lambda\}_{\lambda\in\Lambda}$ is a set of elements in R, then the ideal *generated* by $\{f_\lambda\}_{\lambda\in\Lambda}$ is the smallest ideal containing every f_λ, which we denote by $(f_\lambda)_{\lambda\in\Lambda}$. This ideal is equal to the set of finite R-linear combinations of the f_λ, i.e.,

$$(f_\lambda)_{\lambda\in\Lambda} = \left\{ \sum_{\lambda\in\Lambda'} r_\lambda f_\lambda \;\middle|\; r_\lambda \in R,\ \Lambda' \subseteq \Lambda \text{ finite} \right\}.$$

An ideal $I \subseteq R$ is *principal* if it can be generated by one element.

We define some operations on ideals.

[AK21, (1.4)] [AM69, p. 6]

DEFINITION 1.3.2. Let R be a ring, and let I and J be ideals in R. The *sum* of I and J is

$$I + J \coloneqq \{x + y \in R \mid x \in I,\ y \in J\}.$$

The *intersection* of I and J is

$$I \cap J \coloneqq \{x \in R \mid x \in I,\ x \in J\}.$$

The *product* of I and J is

$$IJ \coloneqq \left\{ \sum_i x_i y_i \;\middle|\; x_i \in I,\ y_i \in J \right\}.$$

All three sets are ideals.

EXAMPLE 1.3.3. We give some examples of operations on ideals. [AM69, p. 6]

(1) In $\mathbf{Z}$, consider the ideals (m) and (n). By prime factorization, we have
$$(m) + (n) = \big(\gcd(m,n)\big),$$
$$(m) \cap (n) = \big(\operatorname{lcm}(m,n)\big),$$
$$(m)(n) = (mn).$$

(2) In the polynomial ring $k[x_1, x_2, \ldots, x_n]$ in n variables over a field k, consider the ideal $I = (x_1, x_2, \ldots, x_n)$. For every integer $m > 0$, the ideal I^m consists of those polynomials with no terms of degree $< m$.

These operations are compatible in the following manner:

LEMMA 1.3.4. *Let R be a ring, and consider three ideals $I, J, K \subseteq R$. Then,* [AK21, (1.4)] [AM69, p. 6]

(i) (distributive law) $I(J + K) = IJ + IK$.

(ii) (modular law) $I \cap (J + K) \supseteq I \cap J + I \cap K$, and equality holds if $I \supseteq J$ or $I \supseteq K$.

Proof. We first show the distributive law. For "$\supseteq$", we have $J \subseteq J + K$ and $K \subseteq J + K$. Multiplying on both sides by I, we therefore have $IJ \subseteq I(J + K)$ and $IK \subseteq I(J+K)$. Now $J+K$ is stable under addition, and hence $IJ+IK \subseteq I(J+K)$. For "$\subseteq$", every element in $I(J + K)$ can be written as
$$\sum_i x_i(y_i + z_i) = \sum_i x_i y_i + \sum_i x_i z_i \in IJ + IK,$$
where $x_i \in I$, $y_i \in J$, and $z_i \in K$.

We now show the modular law. For "$\supseteq$", we have $J \subseteq J + K$ and $K \subseteq J + K$. Intersecting both sides with I, we therefore have $I \cap J \subseteq I \cap (J + K)$ and $I \cap K \subseteq I\cap(J+K)$. Now $J+K$ is stable under addition, and hence $I\cap J+I\cap K \subseteq I\cap(J+K)$. To prove "$\subseteq$", after switching the roles of J and K, we may assume that $I \supseteq J$. Consider an element $x \in I \cap (J + K)$. We can then write $x = y + z$, where $y \in J \subseteq I$ and $z \in K$. We then have
$$x - y = z \in I \cap K,$$
since the left-hand side is in I by the assumption that $y \in J \subseteq I$. Finally, this implies
$$x = y + (x - y) \in J + I \cap K = I \cap J + I \cap K. \qquad \square$$

REMARK 1.3.5. In $\mathbf{Z}$, the equality in the modular law holds even without the assumption that $I \supseteq J$ or $I \supseteq J$. By Example 1.3.3(1), the modular law says that [AM69, p. 6]
$$\operatorname{lcm}\big(\ell, \gcd(m,n)\big) = \gcd\big(\operatorname{lcm}(\ell,m), \operatorname{lcm}(\ell,n)\big).$$

We now consider how ideals interact with ring maps.

DEFINITION 1.3.6. Let $\varphi\colon R \to S$ be a ring map. If $I \subseteq R$ is an ideal, then the ideal IS generated by $\varphi(I)$ in S is the *extension* of I to S. If $J \subseteq S$ is an ideal, then the set $\varphi^{-1}(J)$ is an ideal in R since if $x, y \in \varphi^{-1}(J)$ and $r \in R$, then [AK21, (1.5)] [AM69, p. 2]
$$\varphi(rx + y) = \varphi(r)\,\varphi(x) + \varphi(y) \in J.$$
The ideal $\varphi^{-1}(J)$ is called the *contraction* of J to R. The *kernel* of φ is $\ker(\varphi) \coloneqq \varphi^{-1}(0)$. Note that $\ker(\varphi) = 0$ if and only if φ is injective.

Now consider an arbitrary ideal $I \subseteq R$. We can then consider the *quotient ring*
$$R/I \coloneqq \big\{x + I \;\big|\; x \in R\big\},$$

which is an additive group (the ideal I is an additive subgroup), and admits a ring structure by setting $(x+I)(y+I) = (xy+I)$.

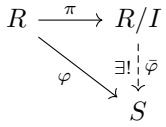
EXAMPLE 1.3.7. To get more comfortable with quotient rings, we want to point out that it is more useful to think of R/I as another ring R' that comes with a surjective ring map $R \to R'$ whose kernel is exactly I. In this way, R/I can be thought of as the ring obtained from R by "imposing the relations in I."

(1) If $R = \mathbf{Z}$ and $I = (n)$ for a positive integer n, then $R/I = \mathbf{Z}/(n)$ is the ring obtained from $\mathbf{Z}$ where we assert that adding 1 to itself n times yields zero. If n is a prime number $p > 0$, then this yields the field $\mathbf{F}_p$ with p elements.
(2) If $R = k[x,y]$ is the polynomial ring in two variables over a field k and $I = (x-y)$, then $R/I = k[x,y]/(x-y)$ is the ring obtained from $k[x,y]$ where we assert that $x - y = 0$, or equivalently $x = y$. Thus, $R/I \simeq k[x]$.

8/21

Quotient rings are characterized by the following universal property:

[AK21, (1.5)] PROPOSITION 1.3.8 (Universal property of quotient rings). *Let R be a ring, and consider an ideal $I \subseteq R$ together with the corresponding quotient map $\pi\colon R \to R/I$. Then, for every ring map $\varphi\colon R \to S$ such that $\varphi(I) = 0$, there exists a unique ring map $\bar{\varphi}\colon R/I \to S$ making the diagram*



commute.

Proof. We first note that a map $\bar{\varphi}$, if it exists, must be unique since π is surjective. It therefore remains to show that $\bar{\varphi}$ exists. We claim setting $\bar{\varphi}(x+I) = \varphi(x)$ is well-defined. If $x' + I = x + I$ in R/I, then $x - x' \in I$, and hence

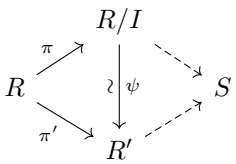
$$\varphi(x') = \varphi(x + x' - x) = \varphi(x) + \varphi(x - x') = \varphi(x).$$

Thus, $\bar{\varphi}(x+I) = \bar{\varphi}(x'+I)$, and $\bar{\varphi}$ is indeed well-defined. The fact that $\bar{\varphi}$ is a ring map then follows by the definition of $\bar{\varphi}$ and the fact that φ is a ring map. □

The power of this universal property comes from the following:

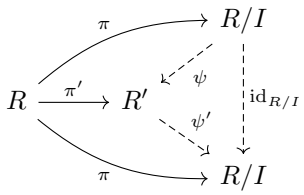
[AK21, (1.5)] COROLLARY 1.3.9. *The universal property in Proposition 1.3.8 determines $\pi\colon R \to R/I$ up to unique isomorphism.*

Proof. We first spell out what the statement means. Suppose $\pi'\colon R \to R'$ is another ring map that satisfies the universal property in Proposition 1.3.8. The assertion is that there exists a unique isomorphism $\psi\colon R/I \to R'$ such that for every ring map $\varphi\colon R \to S$ for which $\varphi(I) = 0$, the diagram

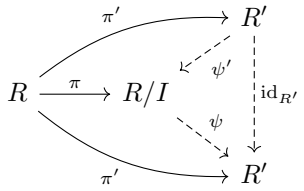


commutes, where the composition $R \to S$ is φ. The existence and uniqueness of ψ comes from the uniqueness of the universal property of R/I (Proposition 1.3.8),

and hence we need to show that ψ is indeed an isomorphism. We can construct the commutative diagram



by applying the universal property (Proposition 1.3.8) for R/I and for R' to the top and bottom triangles in the diagram, respectively. The composition $R/I \to R/I$ is indeed the identity as shown by another application of the universal property for R/I (Proposition 1.3.8), and hence $\psi' \circ \psi = \mathrm{id}_{R/I}$. Switching the roles of R/I and R', we can construct another commutative diagram



and hence $\psi \circ \psi' = \mathrm{id}_{R'}$. □

Remark 1.3.10. The way correct way to state this universal property is: $\pi\colon R \to R/I$ satisfies $\pi(I) = 0$ and is such that for every map $\varphi\colon R \to S$ satisfying $\varphi(I) = 0$, there is a unique map $\bar{\varphi}\colon R/I \to S$ such that $\varphi = \bar{\varphi} \circ \pi$. Another way to state this (see [AK21, (1.5)]) is that $\pi\colon R \to R/I$ is universal among ring maps $\varphi\colon R \to R'$ such that $IR' = 0$.

Remark 1.3.11. Throughout this course, we will prove that various constructions we make satisfy universal properties, which will determine them up to unique isomorphism. While the specific universal property will be different each time, the proof that a universal property uniquely determines the construction up to unique isomorphism will be formally very similar to that of Corollary 1.3.9.

We will soon apply this universal property, but first we note the following:

Proposition 1.3.12. *Let R be a ring, let I be an ideal in R, and let $\pi\colon R \to R/I$ be the corresponding quotient map. There is a bijective inclusion-preserving correspondence* [AK21, (1.8)] [AM69, Prop. 1.1]

$$\left\{\begin{matrix}\text{ideals } J \subseteq R \\ \text{containing } I\end{matrix}\right\} \overset{\text{1-1}}{\longleftrightarrow} \left\{\text{ideals } \bar{J} \subseteq R/I\right\}$$

$$J \longmapsto J/I$$

$$\pi^{-1}(\bar{J}) \longmapsfrom \bar{J}$$

where

$$J/I = \left\{x + I \in R/I \;\middle|\; x \in J\right\} = \pi(J).$$

Moreover, we have $J/I = J(R/I)$.

Proof. We note that $\pi(J)$ is an ideal in R/I since if $\bar{x}, \bar{y} \in \pi(J)$ and $\bar{r} \in R/I$, then

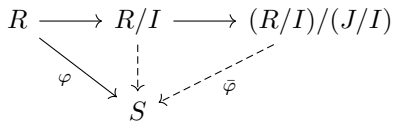
$$\bar{r}\bar{x} + \bar{y} = \pi(r)\,\pi(x) + \pi(y) = \pi(rx + y) \in \pi(J)$$

where $x, y \in J$ and $r \in R$ are elements mapping to x, y, and r under π, respectively. The fact that $\pi(J) = J(R/I)$ then follows since $J(R/I)$ is the smallest ideal containing $\pi(J)$ by definition. The maps in either direction are inclusion-preserving by definition, and are inverses to each other since I is exactly the kernel of π. □

We then have the following isomorphism theorem:

[AK21, (1.5)] THEOREM 1.3.13. *Let R be a ring, and let I be an ideal in R. For every ideal $J \subseteq R$ containing I, the universal property in Proposition 1.3.8 induces a unique isomorphism $R/J \simeq (R/I)/(J/I)$.*

Proof. By Corollary 1.3.9, it suffices to show that $(R/I)/(J/I)$ satisfies the universal property for R/J. Let $\varphi\colon R \to S$ be a ring map such that $\varphi(J) = 0$. We want to show that there is a unique ring map $\bar{\varphi}$ making the diagram



commute. The vertical arrow $R/I \to S$ exists and is unique by the universal property for $R \to R/I$, and maps J/I to 0. The map $\bar{\varphi}$ therefore exists by the universal property for $R/I \to (R/I)/(R/J)$, where we use the fact that J/I is an ideal by Proposition 1.3.12, which maps to 0 in S. □

1.4. Radical, prime, and maximal ideals

Prime ideals are very important for understanding the structure of rings. We will soon see that deciding whether certain ideals are prime, or equivalently whether certain rings are domains, is surprisingly difficult.

We start by defining radical ideals.

[AK21, (3.20)] DEFINITION 1.4.1. Let R be a ring, and let $I \subseteq R$ be an ideal. The *radical* of I is the ideal

$$\sqrt{I} \coloneqq \left\{x \in R \,\middle|\, x^n \in I \text{ for some integer } n > 0\right\}.$$

This is an ideal since if $x^n \in I$, then $(rx)^n \in I$, and if $x^n, y^m \in I$, then

$$(x+y)^{n+m-1} = \sum_{i+j=n+m-1} \binom{n+m-1}{j} x^i y^j \in I$$

by the pigeon-hole principle: if both $i \leq n-1$ and $j \leq m-1$, then $i+j \leq n+m-2$. Note that $I \subseteq \sqrt{I}$ by setting $n = 1$ in the definition.

An ideal $I \subseteq R$ is *radical* if $I = \sqrt{I}$. This is equivalent to saying that if $x^n \in I$ for some integer $n > 0$, then $x \in I$.

DEFINITION 1.4.2. A ring R is *reduced* if (0) is a radical ideal, or in other words, if $x^n = 0$ for some integer $n > 0$ implies $x = 0$.

PROPOSITION 1.4.3. *Let R be a ring. An ideal $I \subseteq R$ is radical if and only if R/I is reduced.*

Proof. $\Rightarrow$. Let $\bar{x} \in R/I$ be an element such that $\bar{x}^n = 0$ for some $n > 0$. Choosing an element $x \in R$ such that x maps to $\bar{x}$ under the quotient map, we have $x^n \in I$. Now since I is radical, we see that $x \in I$, and hence $\bar{x} = 0$.

$\Leftarrow$. Let $x \in R$ be such that $x^n \in I$ for some $n > 0$. Then, $\bar{x}^n = \overline{x^n} = 0$ in R/I. Since I is reduced, we see that $\bar{x} = 0$ in R/I, and hence $x \in I$. □

We now define prime ideals.

DEFINITION 1.4.4. Let R be a ring. [AK21, (2.2), (2.3)] [Hoc17, p. 12] [AM69, p. 3]

(1) A proper ideal $I \subseteq R$ is *prime* if for every pair of elements $x, y \in R$, if $xy \in I$, then $x \in I$ or $y \in I$.
(2) A *multiplicative set* $W \subseteq R$ is a set containing 1 that is closed under multiplication.
(3) We say that R is a *domain* if R is nonzero and if for every pair of elements $x, y \in R$, if $xy = 0$, then either $x = 0$ or $y = 0$.

We now review one of the problems from Homework 0.

PROPOSITION 1.4.5. *Let R be a ring, and consider an ideal $I \subseteq R$. Then, the following are equivalent:*

(*i*) *I is a prime ideal.*
(*ii*) *R/I is a domain.*
(*iii*) *$R - I$ is a multiplicative set.*

Proof. (*i*) $\Rightarrow$ (*ii*). Since I is a proper ideal, we have $R/I \neq 0$. Now suppose $\bar{x}\bar{y} = 0$. Then, $\overline{xy} = 0$, and hence $xy \in I$ where x and y are elements in R mapping to x and y, respectively. Since I is prime, we have $x \in I$ or $y \in I$, and hence $\bar{x} = 0$ or $\bar{y} = 0$.

(*ii*) $\Rightarrow$ (*i*). Since $R/I \neq 0$, we see that I is a proper ideal. Now consider $x, y \in R$ such that $xy \in I$. Then, $\bar{x}\bar{y} = 0$ in R/I, and since R/I is a domain, we have $\bar{x} = 0$ or $\bar{y} = 0$. But this implies $x \in I$ or $y \in I$ since the kernel of $R \to R/I$ is I.

(*i*) $\Leftrightarrow$ (*iii*). We have that I is a proper ideal if and only if $1 \notin R$, which holds if and only if $1 \in R - I$. Now the equivalence (*i*) $\Leftrightarrow$ (*iii*) follows by the fact that "$x \in R - I$ and $y \in R - I \Rightarrow xy \in R - I$" is the contrapositive of "$x \in I$ or $y \in I \Leftarrow xy \in I$." □

We then have:

COROLLARY 1.4.6. *Prime ideals are radical.*

Proof. By Propositions 1.4.3 and 1.4.5, it suffices to note that domains are reduced. □

COROLLARY 1.4.7. *Let $\varphi\colon R \to S$ be a ring map. For every radical (resp. prime) ideal $I \subseteq S$, the contraction $\varphi^{-1}(I)$ is radical (resp. prime).*

In other words, Spec defines a contravariant functor from commutative rings to sets.

Proof. By definition of the kernel, we have an inclusion $R/\varphi^{-1}(I) \hookrightarrow S/I$. Since S/I is reduced (resp. a domain) by Proposition 1.4.3 (resp. Proposition 1.4.5), we see that $R/\varphi^{-1}(I)$ is reduced (resp. a domain), and hence $\varphi^{-1}(I)$ is radical (resp. prime) again by Proposition 1.4.3 (resp. Proposition 1.4.5). □

In Homework 1, you will be showing that the kernel of the map

$$\begin{aligned} \varphi\colon k[w,x,y,z] &\longrightarrow k[s,t] \\ w &\longmapsto s^3 \\ x &\longmapsto s^2t \\ y &\longmapsto st^2 \\ z &\longmapsto t^3 \end{aligned}$$

defining the *twisted cubic curve* is prime, since $k[w,x,y,z]/\ker(\varphi)$ is isomorphic to the image of φ, and is a domain since it is contained in $k[s,t]$. For more complicated ideals, however, it becomes very hard to decide whether it is prime. The following problem is open:

Conjecture 1.4.8 (M. Artin and M. Hochster (1982) [Kad18, Conjecture 1]). [Hoc17, pp. 5–6] *Let k be a field. Consider the polynomial ring $k[\{x_{ij}\}_{1\le i,j\le n}, \{y_{ij}\}_{1\le i,j\le n}]$ in $2n^2$ variables. Let X be the $n\times n$ matrix with entries x_{ij}, and similarly for Y. Then, the ideal*

$$J = \big(\text{the } n^2 \text{ entries of the matrix } XY - YX\big)$$

is prime.

Note that the entries of the matrix $XY - YX$ are all quadratic. It is known that it would suffice to show that the ideal J is in fact radical [Ger61, Chapter II, Theorem 1]. Thompson showed that Conjecture 1.4.8 holds for $n \le 3$ [Tho86].

8/23

We give the set of prime ideals a name.

Definition 1.4.9. The *spectrum* $\operatorname{Spec}(R)$ of R is the set of prime ideals in R.

We now define a smaller class of ideals.

[AK21, (2.12)] [Hoc17, p. 12] Definition 1.4.10. Let R be a ring. A proper ideal $I \subseteq R$ is *maximal* if for every proper ideal $J \supseteq I$, we have $J = I$. The *maximal spectrum* $\operatorname{MaxSpec}(R)$ of R is the set of maximal ideals in R.

Recall that a field is a ring such that $1 \neq 0$ and such that every nonzero element has a multiplicative inverse. We have the following fact about fields:

[AK21, (2.14)] Proposition 1.4.11. *Let R be a ring. Then, k is a field if and only if (0) is a maximal ideal.*

Proof. Suppose $I \supsetneq (0)$, in which case I contains a nonzero element x. Since k is a field, there exists an element $x^{-1} \in k$ such that $x^{-1}x = 1$. But by the assumption that I is an ideal, we see that $1 \in I$, and hence $I = k$.

Conversely, suppose (0) is a maximal ideal. Let $x \in k$ be a nonzero element. Then, $(x) \supsetneq (0)$, and hence $R = (x)$, and hence $1 \in (x)$. By the definition of the ideal generated by an element, this implies there exists an element $x^{-1} \in R$ such that $x^{-1}x = 1$. □

We then have:

[AK21, (2.16)] Corollary 1.4.12. *Let R be a ring, and let I be an ideal. Then, I is maximal if and only if R/I is a field.*

Proof. We see that I is maximal in R if and only if the zero ideal in (0) is maximal in R/I by Proposition 1.3.12. The statement then follows from Proposition 1.4.11. □

Since all fields are domains, combining Proposition 1.4.5 and Corollary 1.4.12 yields:

COROLLARY 1.4.13. *Every maximal ideal is prime, i.e.,* $\mathrm{MaxSpec}(R) \subseteq \mathrm{Spec}(R)$.

On the other hand, the contraction of a maximal ideal is not maximal: consider the inclusion $\mathbf{Z} \subseteq \mathbf{Q}$.

EXAMPLE 1.4.14. Here are some examples.

(1) The prime ideals of $\mathbf{Z}$ are (0) and (p) for primes $p > 0$. Of these, all but (0) are maximal.
(2) The prime ideals of $k[x]$ are (0) and the principal ideals generated by prime (equivalently, irreducible since $k[x]$ is a UFD) elements in $k[x]$. Of these, all but (0) are maximal. If k is algebraically closed, these ideals are of the form $(x - a)$ for $a \in k$.

1.5. Zorn's lemma and applications to prime ideals

We said earlier that we want to study rings by studying prime ideals inside of them. This doesn't make sense unless we actually have prime ideals to work with, and so we will spend some time proving this.

DEFINITION 1.5.1. Let S be a partially ordered set, i.e., there is a relation $\leq$ on S that is reflexive ($x \leq x$ for every x) and transitive ($x \leq y$ and $y \leq z$ implies $x \leq z$), and is such that if $x \leq y$ and $y \leq x$, then $x = y$. A subset $T \subseteq S$ is a *chain* if either $x \leq y$ or $y \leq x$ for every pair of elements $x, y \in T$. Given a subset $T \subseteq S$, an *upper bound* for T is an element $u \in S$ such that $t \leq u$ for every $t \in T$. [Rei95, (1.7)]

The main ingredient is the following result, which is usually known as Zorn's lemma, but was shown by Kuratowski thirteen years earlier.

LEMMA 1.5.2 [Kur1922; Zor35]. *Let S be a nonempty partially ordered set. If every chain in S has an upper bound in S, then S has at least one maximal element.* [Rei95, (1.7)]

REMARK 1.5.3. We will not prove Lemma 1.5.2. The assertion "every ring has a maximal ideal" is equivalent to the axiom of choice assuming the axioms of Zermelo–Frankel set theory.

We use Lemma 1.5.2 to show:

THEOREM 1.5.4. *Let $I \subseteq R$ be a proper ideal. Then, I is contained in a maximal ideal in R.* [AK21, (2.28)] [Rei95, (1.8)]

Proof. We apply Zorn's lemma (Lemma 1.5.2) to the partially ordered set of proper ideals containing I, with the partial order given by inclusion. To do so, we have to show that every chain of proper ideals containing I has an upper bound for the chain. If $\{J_\lambda\}_{\lambda \in \Lambda}$ is a chain of proper ideals containing I, then we claim that

$$J = \bigcup_{\lambda \in \Lambda} J_\lambda$$

is a proper ideal containing I. The fact that J contains I holds since every J_λ contains I. Now if $x, y \in J$, then $x, y \in J_\lambda$ for some $\lambda \in \Lambda$, and hence $rx + y \in J_\lambda \subseteq J$ for every $r \in R$. Lastly, $1 \notin J$ since it is not contained in any of the J_λ. □

We can strengthen Theorem 1.5.4 in the following way:

PROPOSITION 1.5.5. *Let R be a ring, let $W \subseteq R$ be a multiplicative set, and let $I \subseteq R$ be an ideal disjoint from W. Then, there exists a prime ideal $P \subseteq R$ containing I and disjoint from W.* [AK21, (3.10)] [Rei95, (1.9)]

Proof. Suppose $P \supseteq I$ is an ideal maximal subject to the condition $P \cap W = \emptyset$. We claim that P is prime. We show this by showing that $R - P$ is multiplicative; note that $1 \in R - P$ automatically since $1 \in W$, and hence it remains to show that $R - P$ is closed under multiplication. If $x, y \in R - P$, then $P + (x)$ and $P + (y)$ are strictly larger than P, and hence intersect W. We therefore see that there exist $p, q \in P$ such that $p + rx \in W$ and $q + sy \in W$ for some $r, s \in R$. Since W is multiplicative,

$$(p + rx)(q + sy) = pq + psy + qrx + rsxy \in W.$$

But $pq + psy + qrx \in P$, and hence we must have $xy \in R - P$.

It therefore remains to show that such an ideal P exists. Let S be the set of ideals containing I and disjoint from W. Given a chain of ideals $\{J_\lambda\}$ in S, set $J = \bigcup J_\lambda$. This is an upper bound for this chain. □

This has the following corollary:

[Rei95, (1.10)]

COROLLARY 1.5.6. *Let R be a ring. Then, we have*

$$\sqrt{(0)} = \bigcap_{P \subsetneq R \text{ prime}} P.$$

Proof. We first show the inclusion $\subseteq$. Recall that prime ideals are radical (Corollary 1.4.6). Since $0 \in P$, if $f^n = 0$, we also have $f \in P$, showing $\subseteq$.

For the inclusion $\supseteq$, we prove the contrapositive. Suppose $f \notin \sqrt{(0)}$. There then exists a prime P disjoint from $W = \{1, f, \ldots, f^n, \ldots\}$ by Proposition 1.5.5. We therefore have $f \notin P$, and hence $f \notin \bigcap_{P \in \mathrm{Spec}(R)} P$. □

We can now show:

[AK21, (3.27)] [Rei95, (1.12)]

THEOREM 1.5.7 ("Scheinnullstellensatz"). *Let R be a ring. For every ideal I, we have*

$$\sqrt{I} = \bigcap_{\substack{P \subsetneq R \text{ prime} \\ P \text{ contains } I}} P = \bigcap_{\substack{P \subsetneq R \text{ prime} \\ P \text{ minimal over } I}} P$$

Proof. The second equality follows from Zorn's lemma, since every prime ideal containing I contains a minimal prime over I by Zorn's lemma (see [AK21, (3.12)]): if there is a chain of ideals containing I ordered with respect to (reverse) inclusion, then the intersection of these ideals is prime and is an upper bound for this chain. The first equality follows from Corollary 1.5.6, and the fact that under the correspondence of Proposition 1.3.12, prime ideals correspond to prime ideals (quotienting on either side gives the same result). Alternatively, one could prove this directly using Proposition 1.5.5. □

We then have the following:

COROLLARY 1.5.8. *Let R be a ring. Then, R is reduced if and only if the ring map*

$$R \longrightarrow \prod_{\substack{P \subsetneq R \\ P \text{ minimal prime}}} R/P$$

mapping r to the element in the product whose P-th coordinate is the image of r in R/P is an injective map.

Proof. By the Scheinnullstellensatz (Theorem 1.5.7), the kernel of this map is $\sqrt{(0)}$. □

1.6. Spectra as topological spaces

Last time, we saw the definition of the spectrum of a ring, and proved that it is nonempty if and only if the ring is nonzero. We will now study its structure in a bit more depth.

The first goal will be to show that $\operatorname{Spec}(R)$ has the structure of a topological space. We recall the definition of a topological space here:

DEFINITION 1.6.1. Let X be a set. A *topology* on X is a collection $\mathcal{F}$ of subsets of X called *closed sets* satisfying the following properties: [Mun00, p. 76]

(1) $\emptyset, X \in \mathcal{F}$;
(2) $\mathcal{F}$ is closed under arbitrary intersections; and
(3) $\mathcal{F}$ is closed under finite unions.

A set X for which a toplogy $\mathcal{F}$ has been specified is called a *topological space*. A subset $U \subseteq X$ is an *open set* if its complement is closed.

Given a subset $A \subseteq X$, the *closure* of A in X is the smallest closed subset $\overline{A} \subseteq X$ containing A.

We now define a topology on $\operatorname{Spec}(R)$.

DEFINITION 1.6.2. Let R be a ring. The *Zariski topology* on $\operatorname{Spec}(R)$ is defined by saying the closed sets are [AK21, (13.1)]

$$V(I) \coloneqq \big\{P \in \operatorname{Spec}(R) \,\big|\, I \subseteq P\big\},$$

where I runs over all ideals $I \subseteq R$. To check this defines a topology, we need to show that the $V(I)$ satisfy the axioms above:

(1) $V(0) = \operatorname{Spec}(R)$ and $V(1) = \emptyset$.
(2) Let $\{I_\lambda\}_{\lambda\in\Lambda}$ be a collection of ideals. Then, an ideal contains every I_λ if and only if it contains $\sum_{\lambda\in\Lambda} I_\lambda$ since ideals are closed under addition, and hence
$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V\left(\sum_{\lambda\in\Lambda} I_\lambda\right).$$
(3) Let I and J be ideals, and let P be an ideal. Then, the following are equivalent: [AK21, (2.2)]
   (i) $I \subseteq P$ or $J \subseteq P$;
   (ii) $I \cap J \subseteq P$;
   (iii) $IJ \subseteq P$.
   and hence
   $$V(I) \cup V(J) = V(I \cap J) = V(IJ).$$
   To see that these three conditions are equivalent, we first note (i) ⇒ (ii) follows from the fact that $I \cap J$ is contained in whichever ideal is contained in P. Then, (ii) ⇒ (iii) follows from the fact that $IJ \subseteq I \cap J$. Finally, we show (iii) ⇒ (i) by contrapositive. Suppose $I \not\subseteq P$ and $J \not\subseteq P$. Then, there exist $x \in I - P$ and $y \in J - P$ such that $xy \in IJ - P$.

Finally, open sets of the form

$$D(f) \coloneqq \operatorname{Spec}(R) - V(f)$$

for elements $f \in R$ are called *principal open sets*.

Let us prove one fact about these closed sets.

PROPOSITION 1.6.3. *Let R be a ring. Then, $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.*

In other words, the topology of $\operatorname{Spec}(R)$ only detects ideals up to radical.

Proof. This follows from the Scheinnullstellensatz (Theorem 1.5.7). □

We can now think about our examples from before.

EXAMPLE 1.6.4.

(1) Let $R = \mathbf{Z}$. Then, every ideal $(p) \subseteq R$ for a prime $p > 0$ is maximal. Thus, $V(p) = \{(p)\}$, and hence the points (p) are closed. The point (0) is special: the closure of (0) is all of $\operatorname{Spec}(\mathbf{Z})$! This is a point we call the *generic point*.
(2) Let $R = \mathbf{C}[x]$. Since every ideal in R is principal, i.e., generated by one element, we can write every prime ideal as $P = (f)$, where $f \in \mathbf{C}[x]$ is prime. As before, we can have $f = 0$ in which case $P = (0)$ is the generic point of $\operatorname{Spec}(R)$. If $f \neq 0$, then we can write f as a product of linear polynomials, since $\mathbf{C}$ is algebraically closed. The primeness of $P = (f)$ then forces $f = x - a$ for some $a \in \mathbf{C}$.
(3) Let $R = \mathbf{R}[x]$. We claimed last time that the irreducible polynomials in $\mathbf{R}[x]$ are linear of the form $x - a$, or quadratic and irreducible. To see this, it suffices to show that arbitrary $f \in \mathbf{R}[x]$ can be written as a product of linear and quadratic polynomials. We first factor out all the roots of f over $\mathbf{C}$ to write f as a product of linear polynomials $x - a$ for $a \in \mathbf{C}$. The linear factors therefore can be grouped into conjugate pairs, and hence the polynomials
$$(x - a)(x - \bar{a}) = x^2 - 2\operatorname{Re}(a) + |a|^2$$
are quadratic factors of f. We therefore see that $\operatorname{Spec}(R)$ has a generic point, and a bunch of closed points in bijection with the upper half plane $\mathbf{H} \coloneqq \{a \in \mathbf{C} \mid \operatorname{Im}(a) \geq 0\}$.

We now consider a harder example, which requires some more knowledge from abstract algebra.

[AK21, (2.26)]
[Rei95, (1.5)]

THEOREM 1.6.5. *Let R be a PID (principal ideal domain), and consider the polynomial ring $R[x]$ in one variable over R. Let $P \subseteq R[x]$ be a prime ideal.*

(i) $P = (0)$, or $P = (f)$ with f prime, or P is maximal.
(ii) If P is maximal, then either $P = (f)$ with f prime, or $P = (p, g)$ for $p \in R$ prime and $g \in R[x]$ such that its image in $(R/(p))[x]$ is prime.

See Figure 1.1 for pictures.

Proof. Suppose $P \neq (0)$ and P is not principal. Then, there exist two polynomials $f_1, f_2 \in P$ with no common factor. After possibly replacing f_1 and f_2 by prime factors (which lie in P by the assumption that P is prime), we may assume that

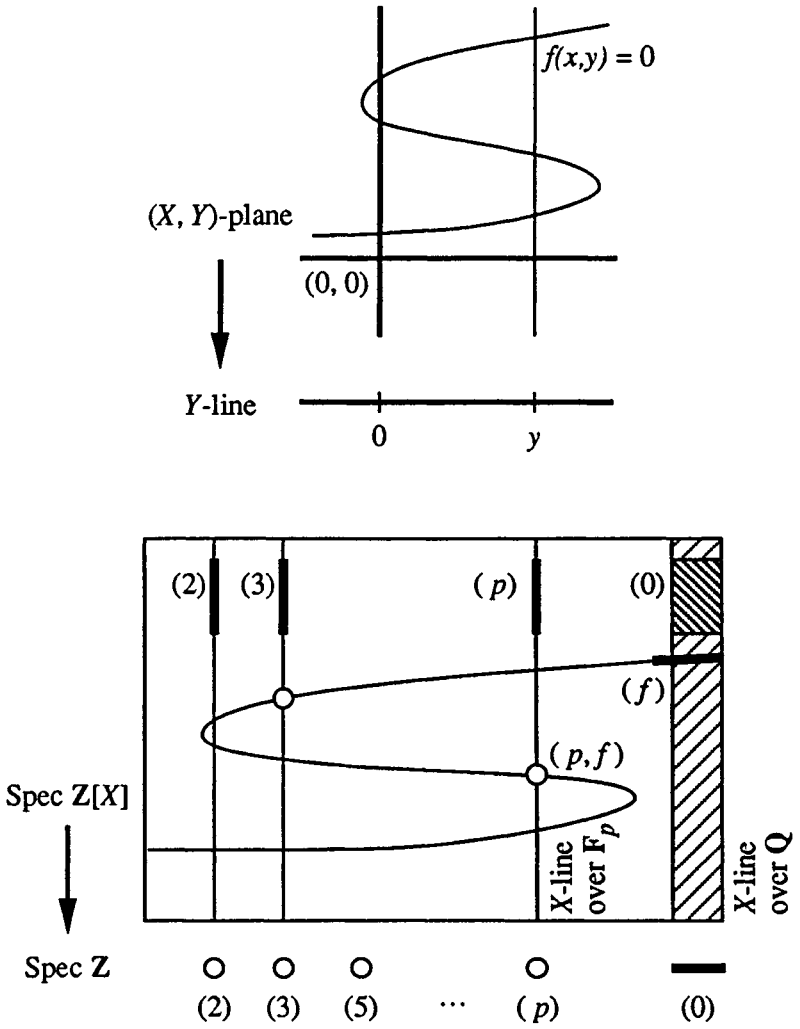


FIGURE 1.1. Spec($k[X,Y]$) and Spec($\mathbf{Z}[Y]$). From [Rei95, p. 24].

f_1 and f_2 are prime. Set K to be the fraction field of R, i.e., the field obtained from R by adjoining an inverse for every nonzero element in R. Gauss's lemma implies that f_1 and f_2 are relatively prime in $K[x]$. Since $K[x]$ is a PID, there exist $h_1, h_2 \in K[x]$ such that $h_1 f_1 + h_2 f_2 = 1$. Clearing denominators gives $P \cap R \neq 0$. Since R is a PID, we have $P \cap R = (p)$ for a prime element $p \in R$.

Now set $k \coloneqq R/(p)$, which is a field. Set $Q = P(R[x]/(p)) \subseteq (R[x])/(p) \simeq k[x]$, where this isomorphism holds by the universal property of quotient rings [AK21, (1.6)]. The fact about quotient rings from last time shows that $k[x]/Q = R[x]/P$. Now since P is prime, these rings are domains, and hence we have $Q = \langle g' \rangle$, where $g' \in k[x]$ is prime. Moreover, $k[x]/Q$ is a field since Q is in fact a maximal ideal by the fact that $k[x]$ is a PID. Now choosing $g \in R[x]$ mapping to g' under the quotient map $R[x] \to k[x]$, we are done. □

1.7. Product rings and their spectra

8/26

We now recall the example from Homework 0.

[AK21, (2.11)] Proposition 1.7.1. *Let R and S be rings. Then, the prime (resp. maximal) ideals of R are of the form $I \times S$ or $R \times J$, where $I \subseteq R$ and $J \subseteq S$ are prime (resp. maximal) ideals.*

We will need:

[AK21, (1.15)] Lemma 1.7.2. *The ideals in $R \times S$ are of the form $I \times J$, where $I \subseteq R$ and $J \subseteq S$ are ideals. Moreover, $(R \times S)/(I \times J) \simeq (R/I) \times (S/J)$.*

Proof. Note that every set $I \times J$ of this form is an ideal, since multiplication is computed component-wise. Now if $K \subseteq R \times S$ is an arbitrary ideal, set

$$I \coloneqq \{x \in R \mid (x, 0) \in K\} \qquad \text{and} \qquad J \coloneqq \{y \in S \mid (0, y) \in K\}.$$

Both I and J are ideals, again since multiplication is computed component-wise. By definition, we have $K \supseteq I \times 0 + 0 \times J = I \times J$. Conversely, if $(x, y) \in K$, then $x = (1, 0) \cdot (x, y) \in K$ and $y = (0, 1) \cdot (x, y) \in K$, and hence $(x, y) \in I \times J$. The "moreover" statement follows by definition of quotient rings. □

We can now prove Proposition 1.7.1.

Proof of Proposition 1.7.1. Ideals of this form are prime (resp. maximal) by the description of the quotient ring in Lemma 1.7.2 and then by Proposition 1.4.5 and Corollary 1.4.12. It remains to show that every prime (resp. maximal) ideal must be of this form. By Lemma 1.7.2, the ideals in $R \times S$ are of the form $I \times J$. Since $I \times J$ is prime (resp. maximal), we see that $R/I \times S/J$ is a domain (resp. field). We see that either $I = R$ or $J = S$, for otherwise $(1, 0) \cdot (0, 1) = 0$. Applying Proposition 1.4.5 and Corollary 1.4.12 again, we see that $I \times J$ must be of the form desired. □

Proposition 1.7.1 enables us to show what spectra of products of rings look like.

[AK21, (13.3)] Proposition 1.7.3. *Let R be a ring. Then, $X = \operatorname{Spec}(R)$ can be written as a disjoint union of two open subsets if and only if $R \simeq R_1 \times R_2$.*

The condition that $\operatorname{Spec}(R)$ can be written as a disjoint union of two open subsets is the same as saying $\operatorname{Spec}(R)$ is not connected.

Proof. For $\Leftarrow$, it suffices to note that

$$\operatorname{Spec}(R_1 \times R_2) = V\big((1, 0)\big) \amalg V\big((0, 1)\big)$$

by Proposition 1.7.1. Both of these sets are complements of closed sets, hence also open. We now show $\Rightarrow$. Suppose $X = U_1 \amalg U_2$. Then, U_1 and U_2 are also closed, and hence $U_1 = V(I_1)$ and $U_2 = V(I_2)$. We have

$$V(0) = X = U_1 \cup U_2 = V(I_1 \cdot I_2),$$

which implies $I_1 I_2 \subseteq \sqrt{(0)}$. Similarly,

$$V(R) = \emptyset = U_1 \cap U_2 = V(I_1 + I_2),$$

which implies $\sqrt{I_1 + I_2} = R$ by Proposition 1.6.3. But $1 \in \sqrt{I_1 + I_2}$ implies that $1 \in I_1 + I_2$, since $1^n = 1$ for every integer $n > 0$, and hence we can find elements

$x_1 \in I_1$ and $x_2 \in I_2$ such that $x_1 + x_2 = 1$. Now choose d such that $(x_1x_2)^d = 0$, which exists since $I_1I_2 \subseteq \sqrt{\langle 0 \rangle}$. We can expand $(x_1 + x_2)^{2d-1}$ to write

$$\begin{aligned} 1 &= (x_1 + x_2)^{2d-1} \\ &= \underbrace{x_1^{2d-1} + \binom{2d-1}{1} x_1^{2d-2}x_2 + \cdots + \binom{2d-1}{d} x_1^d x_2^{d-1}}_{e_1} \\ &\quad + \underbrace{\binom{2d-1}{d-1} x_1^{d-1}x_2^d + \binom{2d-1}{d-2} x_1^{d-2}x_2^{d+1} + \cdots + x_2^{2d-1}}_{e_2} \end{aligned}$$

We then have $e_1e_2 = 0$ since every term in the is divisible by $(x_1x_2)^d$, and we have $e_i^2 = 0$ for $i \in \{1, 2\}$ since $e_1^2 = e_1(1 - e_2) = e_1$ and similarly for $i = 2$. This gives a pair of complementary idempotents as defined in [AK21, (1.10)]. Here, idempotent means that $e_i^2 = e_i$ for $i \in \{1, 2\}$, and complementary means that $e_1e_2 = 0$. Now consider the map

$$\begin{aligned} \varphi \colon R &\longrightarrow (e_1) \times (e_2) \\ r &\longmapsto (re_1, re_2) \end{aligned}$$

This is a ring map, since it is additive by the ring axioms, and is multiplicative since

$$\varphi(rs) = (rse_1, rse_2) = (rse_1^2, rse_2^2) = (re_1, re_2)\,(se_1, se_2) = \varphi(r)\,\varphi(s).$$

Finally, φ is surjective since $(re_1, se_2) = \varphi(re_1 + se_2)$, and is injective since if $re_1 = re_2 = 0$, then $r = r(e_1 + e_2) = re_1 + re_2 = 0$. □

1.8. Hartshorne's conjecture

Before we move on, I want to discuss one aspect about the twisted cubic curve from Homework 1. In that problem, I asked you to prove that an ideal is prime and to find two elements generating that prime ideal up to radical. You may be wondering if there is a systematic way of doing this. While there is a systematic way of proving that ideals in polynomial rings are prime using Gröbner bases (this can even be verified by computer), there is no systematic way of finding generators of an ideal up to radical! This is exemplified by:

Open Problem 1.8.1 [Har70, Exercise III.5.16]. *Let k be a field of characteristic zero (i.e., containing the rational numbers $\mathbf{Q}$), and consider the ring homomorphism*

$$\begin{aligned} \varphi \colon k[x, y, z, w] &\longrightarrow k[s, t] \\ w &\longmapsto s^4 \\ x &\longmapsto s^3t \\ y &\longmapsto st^3 \\ z &\longmapsto t^4 \end{aligned}$$

and set $I = \ker(\varphi)$. Can I be generated by two elements up to radical?

Hartshorne in [Har70] asked this question for *homogeneous* equations, although as far as we are aware this version of his question is also open (cf. [Lyu89, Problem 0.1]). It is a special case of what is sometimes called Hartshorne's conjecture, which is an exercise in Harthorne's algebraic geometry textbook; see [Har77, Chapter I,

Exercise 2.17(d)]. Hartshorne showed that Open Problem 1.8.1 has an affirmative answer when k is of positive characteristic [Har79, Theorem].

CHAPTER 2

Modules

An important part of commutative algebra is the study of modules. These are the analogues of vector spaces over fields.

2.1. Categories

Before we start discussing modules and various constructions we will perform on modules, we now take the time to introduce terminology from category theory. These will give us a convenient language to talk about modules and various operations we will perform on them.

DEFINITION 2.1.1. A *category* $\mathcal{C}$ consists of the following data: [AK21, (6.1)] [Hoc17, p. 8]

(1) A class of *objects*.
(2) For every pair of objects A and B in $\mathcal{C}$, a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of *maps* or *morphisms*, such that $\mathrm{Hom}_{\mathcal{C}}(A, B)$ and $\mathrm{Hom}_{\mathcal{C}}(A', B')$ are disjoint unless $A = A'$ and $B = B'$. We write $f\colon A \to B$ to mean that $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.
(3) For every triple of objects A, B, and C in $\mathcal{C}$, a *composition law*

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C) \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

satisfying the following axioms:
   (*a*) For every object B, there is a distinguished *identity* morphism $\mathrm{id}_B\colon B \to B$ such that for every morphism $f\colon A \to B$, we have $\mathrm{id}_A \circ f = f$, and for every morphism $g\colon B \to C$, we have $g \circ \mathrm{id}_B = g$.
   (*b*) Composition is associative: if $f\colon A \to B$, $g\colon B \to C$, and $g\colon C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

We say that $f\colon A \to B$ is a *isomorphism* with inverse $g\colon B \to A$ if $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. If such an inverse exists, it is unique, and is also an isomorphism $g\colon B \to A$. If there is an isomorphism between a pair of objects A and B, we say that A and B are *isomorphic*.

Given a category $\mathcal{C}$, we can construct the *opposite category* $\mathcal{C}^{\mathrm{op}}$. It has the same objects as $\mathcal{C}$, and the morphisms are given by $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$. If $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(B, C)$, then composition is given by $g \circ_{\mathcal{C}^{\mathrm{op}}} f = f \circ_{\mathcal{C}} g$. [Hoc17, p. 11]

EXAMPLE 2.1.2. We give some examples of categories we have already seen in this course. [Hoc17, pp. 9–10]

(1) The category Sets of sets, with functions as morphisms.
(2) The category Rings of (commutative unital) rings, with ring maps as morphisms.
(3) The category Grp of groups, with group homomorphisms as morphisms.

(4) The category Ab of abelian groups, with group homomorphisms as morphisms.
(5) The category Top of topological spaces, with continuous maps (i.e., maps such that the inverse image of every closed set is closed) as morphisms.

So far, objects have underlying sets, morphisms are given by certain functions on those sets, and composition coincides with composition of functions. The following examples are not of this form:

(6) Let $(P, \leq)$ be a partially ordered set. We can consider the category of all elements $x \in P$ where $\mathrm{Hom}(x, y)$ is a set consisting of one element if $x \leq y$, and is empty otherwise. In this category, isomorphic objects are equal.
(7) A category with one object in which every morphism is an isomorphism. This is essentially the same data as a group, where the morphisms of the object correspond to the elements of the group.

The utility of categories is really in relationships between them, given by functors.

Definition 2.1.3. Given two categories $\mathcal{C}$ and $\mathcal{D}$, a *(covariant) functor* $F\colon \mathcal{C} \to \mathcal{D}$ is a rule that assigns to each object A of $\mathcal{C}$ an object $F(A)$ of $\mathcal{D}$, and assigns to each morphism $f\colon A \to B$ in $\mathcal{C}$ a morphism $F(f)\colon F(A) \to F(B)$ in $\mathcal{D}$, such that

[AK21, (6.2)] (1) For all objects A in $\mathcal{C}$, we have $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.
[Hoc17, p. 11] (2) For all morphisms $f\colon A \to B$ and $g\colon B \to C$ in $\mathcal{C}$, we have $F(g \circ f) = F(g) \circ F(f)$.

Note that a functor preserves isomorphisms.

A *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$ is a covariant functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

[Hoc17, pp. 11–12] Example 2.1.4. Here are some examples of functors.

(1) Given any category $\mathcal{C}$, there is an identity functor $\mathrm{id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ that sends objects A to A itself and morphisms f to f itself.
(2) There is an *Abelianization* functor $\mathsf{Grp} \to \mathsf{Ab}$ sending a group G to $G/[G, G]$, where
$$[G, G] \coloneqq \left\{ghg^{-1}h^{-1} \;\middle|\; g, h \in G\right\}$$
is the commutator subgroup.
(3) The composition of two functors is a functor. If both are covariant or both are contravariant, then the composition is covariant. If one is covariant and the other is contravariant, then the composition is contravariant.
(4) Given a category $\mathcal{C}$ whose objects have underlying sets and where composition coincides with composition of functions, there is a *forgetful functor* $\mathsf{Forget}\colon \mathcal{C} \to \mathsf{Sets}$ sending objects to their underlying sets, and morphisms to their underlying functions.
(5) A category $\mathcal{C}$ is a *full subcategory* of another category $\mathcal{D}$ if the objects of $\mathcal{C}$ form a subclass of objects in $\mathcal{D}$, and if $\mathrm{Hom}_{\mathcal{C}}(A, B) = \mathrm{Hom}_{\mathcal{D}}(A, B)$ for every pair of objects A and B in $\mathcal{C}$. For example, finite sets form a full subcategory of Sets, Ab is a full subcategory of Grp.
(6) The spectrum $\mathrm{Spec}(R)$ defines a contravariant functor
$$\mathrm{Spec}\colon \mathsf{Rings}^{\mathrm{op}} \longrightarrow \mathsf{Top}.$$

This is because if $\varphi\colon R \to S$, then we have a map

$$\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$$

by Corollary 1.4.7. This map is continuous since if $V(I) \subseteq \operatorname{Spec}(R)$ is a closed subset, then $(\operatorname{Spec}(\varphi))^{-1}(V(I)) = V(\varphi(I)S)$.

(7) Here is a non-example: Mimicking the definition of $\operatorname{Spec}(\varphi)$ for the maximal spectrum MaxSpec does not define a functor $\mathsf{Rings}^{\mathrm{op}} \to \mathsf{Top}$ (where $\operatorname{MaxSpec}(R)$ is given the subspace topology), or even to Sets, since the inverse image of a maximal ideal is not always maximal. One example of this is $\mathbf{Z} \to \mathbf{Q}$, where the maximal ideal $(0) \subseteq \mathbf{Q}$ has inverse image $(0) \subseteq \mathbf{Z}$, which is not maximal. The same thing occurs for $k[x] \to k(x)$.

We also define natural transformations and isomorphisms of functors.

Definition 2.1.5. Let $F, G\colon \mathcal{C} \to \mathcal{D}$ be two functors. A *natural transformation* $T\colon F \Rightarrow G$ assigns to every object X in $\mathcal{C}$ a morphism $T_X\colon F(X) \to G(X)$ such that for all morphisms $f\colon X \to Y$ in $\mathcal{C}$, there is a commutative diagram [Hoc17, pp. 13–15]

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ {\scriptstyle T_X}\downarrow & & \downarrow{\scriptstyle T_Y} \\ G(X) & \xrightarrow{G(f)} & G(Y). \end{array}$$

Natural transformations $S\colon F \Rightarrow G$ and $T\colon G \Rightarrow H$ can be composed to form the natural transformation $T \star S\colon F \Rightarrow H$ given by the rule

$$(T \star S)_X \coloneqq T_X \circ S_X.$$

There is an identity natural transformation id_F from $F\colon \mathcal{C} \to \mathcal{D}$ to itself. Two functors $F, G\colon \mathcal{C} \to \mathcal{D}$ are *isomorphic* if there are natural transformations

$$T\colon F \Longrightarrow G \qquad \text{and} \qquad T'\colon G \Longrightarrow F$$

such that $T' \star T = \mathrm{id}_F$ and $T \star T' = \mathrm{id}_G$. In fact, T is an isomorphism if and only if the morphisms T_X are isomorphisms for all objects X, in which case

$$(T_X^{-1}) = (T_X)^{-1}.$$

Here is an example.

Example 2.1.6. Let V be a vector space over a field k and write [Hoc17, p. 14]

$$V^* \coloneqq \operatorname{Hom}_k(V, k).$$

Then, $(-)^*$ is a contravariant functor from k-vector spaces Vect_k to Vect_k. Composing $(-)^*$ with itself, we get the covariant functor

$$(-)^{**}\colon \mathsf{Vect}_k \longrightarrow \mathsf{Vect}_k.$$

There is a natural transformation $T\colon \mathrm{id}_{\mathsf{Vect}_k} \Rightarrow (-)^{**}$ defined by

$$\begin{aligned} T_V\colon V &\longrightarrow V^{**} \\ v &\longmapsto \big(g \longmapsto g(v)\big). \end{aligned}$$

To check this defines a natural transformation, we need to check that for every k-linear map $f\colon V \to W$, the diagram

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle T_V}\downarrow & & \downarrow{\scriptstyle T_W} \\ V^{**} & \xrightarrow{f^{**}} & W^{**} \end{array}$$

commutes (this follows from the definition). The map $V \to V^{**}$ is always injective, but may not be an isomorphism. It is an isomorphism for example when V is finite-dimensional.

Using isomorphisms of functors, we can define equivalences of categories.

[Hoc17, p. 15] Definition 2.1.7. Two categories $\mathcal{C}$ and $\mathcal{D}$ are *equivalent* if there exist functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ such that $G \circ F$ is isomorphic to the identity functor on $\mathcal{C}$ and $F \circ G$ is isomorphic to the identity functor on $\mathcal{D}$. Two categories $\mathcal{C}$ and $\mathcal{D}$ are *antiequivalent* if $\mathcal{C}^{\mathrm{op}}$ is equivalent to $\mathcal{D}$.

Another useful notion is that of a *representable functor*.

[Hoc17, pp. 15–16] Definition 2.1.8. Fix an object Z in a category $\mathcal{C}$. Consider the covariant functor

$$\begin{aligned} h^Z\colon \mathcal{C} &\longrightarrow \mathsf{Sets} \\ X &\longmapsto \mathrm{Hom}_{\mathcal{C}}(Z, X) \\ f &\longmapsto f \circ (-). \end{aligned}$$

A covariant functor $G\colon \mathcal{C} \to \mathsf{Sets}$ is *representable* in the category $\mathcal{C}$ if it is isomorphic to h^Z for some object Z in $\mathcal{C}$, in which case we say that Z *represents* G. Similarly, we can consider the contravariant functor

$$\begin{aligned} h_Z\colon \mathcal{C}^{\mathrm{op}} &\longrightarrow \mathsf{Sets} \\ X &\longmapsto \mathrm{Hom}_{\mathcal{C}}(X, Z) \\ f &\longmapsto (-) \circ f \end{aligned}$$

and say that a contravariant functor is *representable* in the category $\mathcal{C}$ if it is isomorphic with h_Z for some object Z in $\mathcal{C}$.

[Hoc17, pp. 16–17] Examples 2.1.9. Representable functors appear very often in commutative algebra and in many other fields.

(*a*) For a fixed group G, consider the functor

$$\begin{aligned} F\colon \mathsf{Ab} &\longrightarrow \mathsf{Sets} \\ A &\longmapsto \mathrm{Hom}_{\mathsf{Grp}}(G, A). \end{aligned}$$

Then, F is representable by the Abelianization $G/[G,G]$ since every map $G \to A$ factors uniquely through $G/[G,G]$, giving a bijection between $F(A)$ and $\mathrm{Hom}_{\mathsf{Grp}}(G/[G,G], A)$. We therefore obtain an isomorphism $F \cong h_{G/[G,G]}$.

(*b*) Let R be a ring and let I be an ideal. Consider the functor

$$\begin{aligned} F\colon \mathsf{Rings} &\longrightarrow \mathsf{Sets} \\ S &\longmapsto \big\{ f\colon R \to S \;\big|\; f(I) = 0 \big\}. \end{aligned}$$

Every map on the right-hand side factors uniquely as $R \twoheadrightarrow R/I \to S$, and hence F is representable by R/I.

(c) (Products) Let $\mathcal{C}$ be a category. Let X and Y be two objects in $\mathcal{C}$. An object Z in $\mathcal{C}$ together with morphisms $\pi_X \colon Z \to X$ and $\pi_Y \colon Z \to Y$ is a *product* for X and Y in $\mathcal{C}$ if, for all objects W in $\mathcal{C}$, the function

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(W, Z) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(W, X) \times \mathrm{Hom}_{\mathcal{C}}(W, Y) \\ f &\longmapsto (\pi_X \circ f, \pi_Y \circ f) \end{aligned}$$

is a bijection, that is, the functor sending W to $\mathrm{Hom}_{\mathcal{C}}(W, X) \times \mathrm{Hom}_{\mathcal{C}}(W, Y)$ is representable in $\mathcal{C}$. The maps π_X and π_Y are called the *projection maps*. By the defining property above, given another product Z' for X and Y with projection maps π'_X and π'_Y, there are mutually inverse isomorphisms $\gamma \colon Z \to Z'$ and $\delta \colon Z' \to Z$ compatible with the projection maps. The fact that the compositions $\gamma \circ \delta$ and $\delta \circ \gamma$ are the identity follow from the defining property of the product.

The product of two objects in $\mathcal{C}^{\mathrm{op}}$ is called their *coproduct* in $\mathcal{C}$.

Note that products do not always exist. For sets, rings, groups, Abelian groups, R-modules, and topological spaces, products do exist and coincide with the usual Cartesian product. However, for other categories this is not the case. For the category associated with a partially ordered set, the product of two elements x and y is the greatest lower bound of x and y, if it exists.

We will return to more notions from category theory every so often as they are needed.

2.2. Definitions of modules

We now define modules. These should be thought of as "Abelian groups with R-actions for rings R." 8/28

Definition 2.2.1. Let R be a ring. An *R-module* is an Abelian group M written additively, together with an R-action $R \times M \to M$, written $(r, m) \mapsto rm$, satisfying the following properties: [AK21, (4.1)]

(1) (distributivity) $r(m + n) = rm + rn$ and $(r + s)m = rm + sm$.
(2) (associativity) $r(sm) = (rs)m$.
(3) (unitariness) $1 \cdot m = m$.

One can show that $r \cdot 0 = 0$ and $0 \cdot m = 0$ for every $r \in R$ and $m \in M$, respectively.

A *map* of R-modules M and N is a map $\varphi \colon M \to N$ of Abelian groups, such that $\varphi(r \cdot m) = r \cdot \varphi(m)$ for every $r \in R$ and $m \in M$. These form a set $\mathrm{Hom}_R(M, N)$, and the class of R-modules with R-module maps forms a category Mod_R.

The set $\mathrm{Hom}_R(M, N)$ is in fact an R-module, where $\varphi + \psi$ and $r \cdot \varphi$ for $r \in R$ are defined by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{and} \qquad (r \cdot \varphi)(m) = r \cdot \big(\varphi(m)\big).$$

If $\varphi \colon M \to N$ is a map of R-modules, the *kernel* and *image* of φ are

$$\ker(\varphi) \coloneqq \varphi^{-1}(0) \subseteq M \qquad \text{and} \qquad \mathrm{im}(\varphi) \coloneqq \varphi(M) \subseteq N,$$

respectively. These subsets of M and N naturally have the structure of R-modules.

Example 2.2.2. $\mathbf{Z}$-modules are the same as abelian groups, and maps of $\mathbf{Z}$-modules are the same as maps of abelian groups. Thus, $\mathsf{Mod}_{\mathbf{Z}}$ and Ab are the same category.

[AK21, (4.1)]

Definition 2.2.3. Let R be a ring. A *submodule* of an R-module M is an abelian subgroup $N \subseteq M$ that is closed under multiplication by R, i.e., for every $r \in R$ and $n \in N$, we have $rn \in N$.

If $I \subseteq R$ is an ideal, then the submodule IM of M is the submodule of M containing all products im with $i \in I$ and $m \in M$.

Example 2.2.4. If R is a ring, the submodules of R are exactly the ideals in R.

[AK21, (4.10)]
[Hoc17, p. 22]

Definition 2.2.5. Let R be a ring, and let M be an R-module. Given a collection of elements $\{m_\lambda\} \subseteq M$, the submodule they *generate* is the smallest submodule of M containing the elements m_λ. A module is *finitely generated* if there is a finite set of generators.

An R-module F is *free* if there exists a set of elements $\mathcal{B} \subseteq F$ called a *free basis* of F that generate M, and such that every element of F can be written *uniquely* as an R-linear combination of elements in $\mathcal{B}$.

The uniqueness here is very important: it says that if $b_1, b_2, \ldots, b_n$ are distinct elements of $\mathcal{B}$ and

$$r_1 b_1 + r_2 b_2 + \cdots + r_n b_n = 0$$

for some elements $r_i \in R$, then necessarily $r_i = 0$ for every i. This is the same condition as linear independence in linear algebra.

Example 2.2.6. If R is a field k, then a module over R is just a k-vector space, and every such module is free, since it has a free basis by Zorn's lemma.

For more general rings, not all modules are free. For example, quotients $\mathbf{Z}/\langle n \rangle$ are not free over $\mathbf{Z}$ for $n \neq 0$, since $n \cdot 1 = 0$ in $\mathbf{Z}/\langle n \rangle$, even though $n \neq 0$ in $\mathbf{Z}$.

Definition 2.2.7. Let R be a ring. Given a collection of R-modules $\{M_\lambda\}_{\lambda \in \Lambda}$, the *direct product* of the M_λ is

$$\prod_{\lambda \in \Lambda} M_\lambda \coloneqq \big\{ (m_\lambda)_{\lambda \in \Lambda} \;\big|\; m_\lambda \in M_\lambda \big\},$$

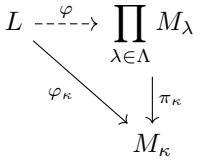
where the R-module structure is given componentwise. The *direct sum* of the M_λ is the sumboddule

$$\bigoplus_{\lambda \in \Lambda} M_\lambda \coloneqq \big\{ (m_\lambda)_{\lambda \in \Lambda} \;\big|\; m_\lambda = 0 \text{ for all but finitely many } \lambda \in \Lambda \big\} \subseteq \prod_{\lambda \in \Lambda} M_\lambda.$$

This inclusion is an equality if Λ is finite.

The direct product comes with projection maps $\pi_\kappa \colon \prod_{\lambda \in \Lambda} M_\lambda \to M_\kappa$ onto the factor M_κ satisfying the following universal property: Given maps $\varphi_\kappa \colon L \to M_\kappa$, there is a unique map $\varphi \colon L \to \prod_{\lambda \in \Lambda} M_\lambda$ making the diagram

(2.2.8)

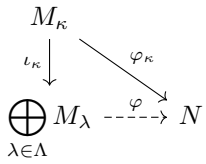


commute. In other words, there is a bijection of sets

$$\mathrm{Hom}_R\Big(L, \prod_{\lambda\in\Lambda} M_\lambda\Big) \xrightarrow{\sim} \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(L, M_\lambda),$$

which is an isomorphism of modules. Similarly, the direct sum comes with injections $\iota_\kappa \colon M_\kappa \to \bigoplus_{\lambda\in\Lambda} M_\lambda$ satisfying the following universal property: Given maps $\varphi_\kappa \colon M_\kappa \to N$, there is a unique map $\varphi \colon \bigoplus_{\lambda\in\Lambda} M_\lambda \to N$ making the diagram

(2.2.9)



commute. In other words, there is a bijection of sets

$$\mathrm{Hom}_R\Big(\bigoplus_{\lambda\in\Lambda} M_\lambda, N\Big) \xrightarrow{\sim} \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M_\lambda, N),$$

which is an isomorphism of modules.

Remark 2.2.10. In an arbitrary category $\mathcal{C}$, the object of $\mathcal{C}$ satisfying the universal property in (2.2.8) (resp. (2.2.9)) for a collection of objects $\{M_\lambda\}_{\lambda\in\Lambda}$, if it exists, is called the *product* (resp. *coproduct*) of that collection. See also Examples 2.1.9(*c*).

With this definition, we can characterize free modules in an alternative fashion:

Lemma 2.2.11. *Let R be a ring, and let M be a module. Then, M is free if and only if there exists an isomorphism $M \xrightarrow{\sim} \bigoplus_{\lambda\in\Lambda} R$ for some indexing set Λ.*

Proof. If there is such an isomorphism, then the images of the standard basis e_λ that is 1 in the λ-th coordinate and zero otherwise in M is a free basis for M. Conversely, if we have a free basis $\{m_\lambda\}_{\lambda\in\Lambda}$ for M, we can define the map by sending m_λ to e_λ as defined above. □

Similarly, one can show:

Lemma 2.2.12. *Let R be a ring, and let M be a module. Then, M is finitely generated if and only if there exists a surjection $\bigoplus_{\lambda\in\Lambda} R \twoheadrightarrow M$, where Λ is a finite set.*

Finally, we want to give some more interesting examples of modules that are not free.

Definition 2.2.13. Let R be a ring, and let M be an R-module. Given an element $m \in M$, the *annihilator* of m is [AK21, (4.1)]

$$\mathrm{Ann}_R(m) \coloneqq \big\{r \in R \,\big|\, rm = 0\big\}.$$

Similarly, the *annihilator* of M is

$$\mathrm{Ann}_R(M) \coloneqq \big\{r \in R \,\big|\, rm = 0 \text{ for every } m \in M\big\}.$$

Both of these are ideals in R.

Now suppose that R is a domain. The *torsion submodule* of M is

$$T(M) \coloneqq \big\{m \in M \,\big|\, \mathrm{Ann}_R(m) \neq 0\big\},$$

and we say that M is *torsion-free* if $T(M) = 0$.

EXAMPLE 2.2.14. The issue in Example 2.2.6 preventing $\mathbf{Z}/\langle n\rangle$ from being a free module is that $1 \in \mathbf{Z}/\langle n\rangle$ is a torsion element. However, not even all torsion-free modules are free: the ideal

$$\langle 2, x\rangle \subseteq \mathbf{Z}[x]$$

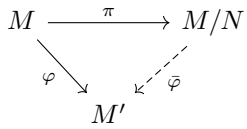
is torsion-free, but is not free. This is because 2 and x both have to be in a generating set (there are no other prime factors of 2 and x), and since the element $2x$ can be written in two ways as a $\mathbf{Z}[x]$-linear combiation of elements in $\langle 2, x\rangle$: $2x = 2 \cdot x = x \cdot 2$.

2.3. Quotient modules

We now discuss how to define quotients of R-modules. We won't prove these results, since the proofs are formally very similar to the proofs we had for quotient rings.

[AK21, (4.6)]

DEFINITION 2.3.1. Let R be a ring, and let M be an R-module. Given a submodule $N \subseteq M$, the *quotient module* M/N is the Abelian group $M/N \coloneqq \{m+N | m \in M\}$ where the R-module structure is given by $r(m+N) = rm + N$. There is a surjective *quotient map* $\pi\colon M \to M/N$ satisfying the following universal property: For every map $\varphi\colon M \to M'$ such that $\varphi(N) = 0$, there is a unique dashed map



making the diagram commute. Using this universal property, one can show that φ induces an isomorphism

$$\frac{M}{\ker(\varphi)} \xrightarrow{\sim} \operatorname{im}(\varphi) \tag{2.3.2}$$

for every map $\varphi\colon M \to N$ of R-modules, that for every chain of inclusions $L \subseteq M \subseteq N$, there is an isomorphism

$$\frac{N}{M} \xrightarrow{\sim} \frac{N/L}{M/L}, \tag{2.3.3}$$

and that for every pair of submodules $L, M \subseteq N$, there is a isomorphism

$$\frac{L}{L \cap M} \xrightarrow{\sim} \frac{L+M}{M}, \tag{2.3.4}$$

where $L + M$ is the submodule of N consisting of all sums $\ell + m$ for $\ell \in L$ and $m \in M$. These isomorphisms (2.3.2), (2.3.3), and (2.3.4) are called Noether's first, second, and third isomorphism theorems, respectively, and were proved in [Noe27].

The *cokernel* and *coimage* of a map $\varphi\colon M \to N$ are

$$\operatorname{coker}(\varphi) \coloneqq \frac{N}{\operatorname{im}(\varphi)} \qquad \text{and} \qquad \operatorname{coim}(\varphi) \coloneqq \frac{M}{\ker(\varphi)}.$$

Note that (2.3.2) implies $\operatorname{coim}(\varphi) \xrightarrow{\sim} \operatorname{im}(\varphi)$.

On Homework 2, you will prove one very useful result about generators of modules versus generators when you pass to a quotient, which is known as Nakayama's lemma (see [Nak51, II]) although Nakayama himself did not like the name. Nakayama instead attributed the result to Krull and Azumaya [Azu51, Theorem 1] in the

commutative case, and to Jacobson [Jac45, Theorem 10] and Azumaya in the non-commutative case [Nag75, p. 213; Mat89, Rem. on p. 8]. Following [Mat89, Thm. 2.2], we will often abbreviate Nakayama's lemma as NAK, to stand for Nakayama–Azumaya–Krull.

NOTATION 2.3.5. Let R be a local ring with unique maximal ideal $\mathfrak{m}$. We will say "$(R, \mathfrak{m}, k)$ is a local ring" to mean that R is a local ring with maximal ideal $\mathfrak{m}$ and with *residue field* $k = R/\mathfrak{m}$.

Here is a variant of what you proved in homework. Note that for a local ring, $\mathfrak{m}$ is equal to the Jacobson radical.

LEMMA 2.3.6 (NAK, version 1). *Let $(R, \mathfrak{m}, k)$ be a local ring and let M be a finitely generated R-module. Then, $M = \mathfrak{m}M$ if and only if $M = 0$.* [AK21, (10.6)] [Hoc17, p. 101] [Hoc07, p. 5]

Proof. The direction $\Leftarrow$ holds since $0 = \mathfrak{m} \cdot 0$. It therefore suffices to show $\Rightarrow$.

Let $u_1, u_2, \ldots, u_h$ be a set of generators for M, where $h > 0$ is minimal. The fact that $M = \mathfrak{m}M$ implies

$$M = \mathfrak{m}u_1 + \mathfrak{m}u_2 + \cdots + \mathfrak{m}u_h.$$

In particular,

$$u_1 = f_1u_1 + f_2u_2 + \cdots + f_hu_h$$

for some $f_i \in \mathfrak{m}$, and hence

$$(1 - f_h)u_1 = f_1u_1 + f_2u_2 + \cdots + f_{h-1}u_{h-1}.$$

Since $1 - f_h$ is a unit (otherwise, Zorn's lemma would show that $1 - f_h \in \mathfrak{m}$ and hence $1 \in \mathfrak{m}$, a contradiction), this shows that u_h is not needed as a generator, contradicting the minimality of h. □

REMARK 2.3.7. If R is not local, the same proof works with $\mathfrak{m}$ replaced by any ideal J contained in the intersection of all maximal ideals in R.

A useful reformulation (also on Homework 2) is the following:

LEMMA 2.3.8 (NAK, version 2). *Let $(R, \mathfrak{m}, k)$ be a local ring, and let M be a finitely generated R-module. If $N \subseteq M$ is a submodule such that $M = N + \mathfrak{m}M$, then $N = M$.* [AK21, (10.8)]

In particular, consider elements $m_1, m_2, \ldots, m_n \in M$. Then, the elements $m_1, m_2, \ldots, m_n$ generate M if and only if their images $\bar{m}_1, \bar{m}_2, \ldots, \bar{m}_n$ span $\bar{M} = M/\mathfrak{m}M$ as a k-vector space.

Proof. The first statement holds by applying NAK version 1 (Lemma 2.3.6) to N/M. We now prove the second statement. $\Rightarrow$ holds since $M \to \bar{M}$ is surjective. For $\Leftarrow$, set $N \coloneqq Rm_1 + Rm_2 + \cdots + Rm_n$. Then, $M = N + \mathfrak{m}M$ and hence $N = M$. □

EXAMPLE 2.3.9. The hypothesis that M is finitely generated is necessary. For a prime number $p > 0$, consider the subring

$$\mathbf{Z}_{(p)} \coloneqq \left\{ \frac{a}{b} \in \mathbf{Q} \;\middle|\; p \nmid b \right\} \subseteq \mathbf{Q},$$

where a and b have no common factors. Then, $\mathbf{Z}_{(p)}$ is a local ring with maximal ideal (p). The $\mathbf{Z}_{(p)}$-module $\mathbf{Q}$ satisfies $\mathbf{Q} = (p) \cdot \mathbf{Q}$, but $\mathbf{Q} \neq 0$.

2.4. Formal power series rings

For later examples, we define formal power series rings here.

[AK21, (3.8)]

EXAMPLE 2.4.1. Let R be a ring. The *formal power series ring* in n variables over R is the ring

$$R[\![x_1, x_2, \dots, x_n]\!] \coloneqq \left\{ \sum_{\nu \in \mathbf{N}^n} r_\nu x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n} \;\middle|\; r_\nu \in R \right\},$$

where the sums are formal infinite sums. For an element in $R[\![x_1, x_2, \dots, x_n]\!]$, the term $r_{(0)} = r_{(0,0,\dots,0)}$ is called its *constant term*. Addition and multiplication are defined in the same way as for polynomials.

Now let $f \in R[\![x_1, x_2, \dots, x_n]\!]$. We claim that f is a unit if and only if its constant term $r_{(0)}$ is a unit. For $\Rightarrow$, if $ff' = 1$, then $r_{(0)} r'_{(0)} = 1$, where $r'_{(0)}$ is the constant term of f'. Conversely, if $r_{(0)}$ is a unit, then $f = r_{(0)}(1 - g)$ with $g \in (x_1, x_2, \dots, x_n)$. We can then set

$$f' \coloneqq r_{(0)}^{-1}(1 + g + g^2 + \cdots),$$

which makes sense since the component of degree d involves only the first $d + 1$ terms. One can check that $ff' = 1$.

Now if $(R, \mathfrak{m})$ is a local ring, then a power series

$$f \notin \mathfrak{m} \cdot R[\![x_1, x_2, \dots, x_n]\!] + (x_1, x_2, \dots, x_n)$$

has constant term $r_{(0)} \notin \mathfrak{m}$, and hence $r_{(0)}$ is a unit by [AK21, (2.29)] (cf. the proof of the NAK Lemma 2.3.6). Thus, f itself is a unit by the previous pagraph, which shows that $R[\![x_1, x_2, \dots, x_n]\!]$ is a local ring with maximal ideal

$$\mathfrak{m} \cdot R[\![x_1, x_2, \dots, x_n]\!] + (x_1, x_2, \dots, x_n)$$

by [AK21, (3.5)].

We want to give an application of the NAK lemma to study formal power series rings. (This was not covered in class.)

EXAMPLE 2.4.2. Consider the formal power series ring version of the twisted cubic curve:

$$\begin{aligned} \varphi \colon k[\![w, x, y, z]\!] &\longrightarrow k[\![s, t]\!] \\ w &\longmapsto s^3 \\ x &\longmapsto s^2 t \\ y &\longmapsto s t^2 \\ z &\longmapsto t^3 \end{aligned}$$

We claim that $I = \ker(\varphi)$ cannot be generated by two elements. Suppose that I can be generated by two elements. We also know that $wx - xy, xz - y^2, wy - x^2 \in I$. These elements are linearly independent over k in the quotient module $I/\mathfrak{m} \cdot I$, and hence cannot generate I by the NAK Lemma 2.3.8.

REMARK 2.4.3. One can rewrite this proof to not use contradiction; I only wrote it this way so that the NAK Lemma 2.3.8 can be applied.

2.5. Exact sequences

We now come to an important concept in commutative algebra and algebra as a whole.

DEFINITION 2.5.1. Let R be a ring. A (finite or infinite) sequence of R-module maps [AK21, (5.1)] [Rei95, (2.9)]

$$\cdots \longrightarrow M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+1} \longrightarrow \cdots$$

is *exact* at M_i if $\ker(\alpha_i) = \operatorname{im}(\alpha_{i-1})$ as submodules of M_i. The sequence is called *exact* if it is exact at every M_i, except at the initial source or final target in the sequence.

EXAMPLE 2.5.2. Here are some special forms of exact sequences. [AK21, (5.2), (5.3)] [Rei95, (2.9), (2.10)]

(1) $0 \to M' \xrightarrow{\alpha} M$ is exact if and only if α is injective.
(2) $M \xrightarrow{\beta} M'' \to 0$ is exact if and only if β is surjective.
(3) A sequence $0 \to M' \xrightarrow{\alpha} M \to M''$ is exact if and only if $M' = \ker(\alpha)$.
(4) A sequence $M' \to M \xrightarrow{\beta} M'' \to 0$ is exact if and only if $M'' = \operatorname{coker}(\beta)$.
(5) A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

(6) A short exact sequence of the form above is *split short exact* if there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \| & & \exists\downarrow\wr & & \| & & \\ 0 & \longrightarrow & M' & \longrightarrow & M' \oplus M'' & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

In a later homework, I will ask you to prove the following:

LEMMA 2.5.3 (Snake). *Consider a commutative diagram* [AK21, (5.12)] [Rei95, Exer. 2.16] [AM69, Prop. 2.10]

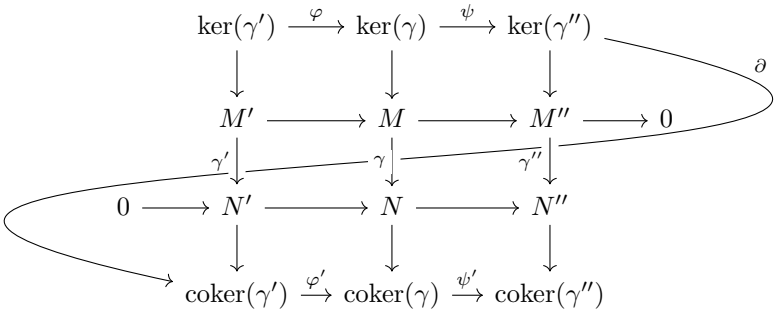
$$\begin{array}{ccccccc} & & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' \longrightarrow 0 \\ & & \gamma'\downarrow & & \gamma\downarrow & & \gamma''\downarrow \\ 0 & \longrightarrow & N' & \xrightarrow{\alpha'} & N & \xrightarrow{\beta'} & N'' \end{array} \tag{2.5.4}$$

with exact rows. Then, there exists an exact sequence

$$\ker(\gamma') \xrightarrow{\varphi} \ker(\gamma) \xrightarrow{\psi} \ker(\gamma'') \xrightarrow{\partial} \operatorname{coker}(\gamma') \xrightarrow{\varphi'} \operatorname{coker}(\gamma) \xrightarrow{\psi'} \operatorname{coker}(\gamma'') \tag{2.5.5}$$

Moreover, if α is injective, then so is φ; dually, if β' is surjective, then so is ψ'.

The reason it is called the Snake Lemma is that the exact sequence (2.5.5) can be visualized as part of (2.5.4):



where the columns are exact. We will keep returning to examples of exact sequences throughout the course.

CHAPTER 3

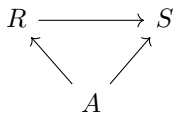
Localization

Our next topic will be localizations, which we can think of as "enlargements" of a ring to contain more multiplicative inverses.

3.1. Algebras

Before we do this, we need the following:

DEFINITION 3.1.1. Let A be a ring. A ring R is an *A-algebra* if R is a A-module that also satisfies the following: if $a \in A$ and $r, s \in R$, then $a(rs) = (ar)s$. A ring R is an A-algebra if and only if there exists a ring map $\theta\colon A \to R$: Given the structure as an A-algebra, we can define $\theta(a) = a \cdot 1_R$, and conversely given θ, we can define the A-module structure by $\theta(a)r$. When R is an A-algebra given by a ring map $\theta\colon A \to R$, we say that θ is the *structure* map. The class of A-algebras form a category Alg_A, where morphisms are ring maps $R \to S$ that are A-linear. This is the same as saying that the diagram [AK21, (1.1)] [Hoc17, p. 18]



commutes, where the arrows from A are the structure maps for R and S, respectively.

We say that S is *finitely generated as an algebra* over R if there exist finitely many elements $x_1, x_2, \ldots, x_r \in S$ such that S is generated by $\varphi(R)$ and the elements $x_1, x_2, \ldots, x_r$ as an algebra.

EXAMPLE 3.1.2.

(1) Every ring R is a $\mathbf{Z}$-algebra in a unique way: there is a unique ring map $\mathbf{Z} \to R$, since $0 \in \mathbf{Z}$ must map to $0 \in R$, $1 \in \mathbf{Z}$ must map to $1 \in R$, repeated addition says that $n \mapsto n \cdot 1_R$ for all positive integers n, and taking additive inverses says that $n \mapsto n \cdot 1_R$ for all negative integers n as well. [Hoc17, p. 19]

Finite generation as a module and as an algebra do not coincide:

(2) The ring $\mathbf{Z}[1/2]$ is finitely generated as an algebra over $\mathbf{Z}$, but not as a module, since it contains $1/2^n$ for every integer n, while any finitely generated submodule of $\mathbf{Z}[1/2]$ consists of fractions whose denominators can be simultaneously cleared by a single power of 2. [Hoc17, p. 29]

(3) The polynomial ring in infinitely many variables over a ring R is not finitely generated as an algebra, since a finite set of generators cannot contain all of the variables.

(4) The field $\mathbf{Q}$ of rational numbers is not finitely generated as a $\mathbf{Z}$-algebra, since any finitely generated subalgebra contains fractions involving only finitely many primes in the denominator.
(5) The ring $\mathbf{Z}[\sqrt{2}]$ is finitely generated as an algebra over $\mathbf{Z}$, and is also finitely generated as a module over $\mathbf{Z}$, since any element can be written $a + b\sqrt{2}$ for $a, b \in \mathbf{Z}$.

To make this distinction more clear, we will say that an A-algebra is *module-finite* if it is finitely generated as an A-module.

3.2. Localization of rings

Recall that a *multiplicative set* W in a ring R is a set containing 1 that is closed under multiplication. The idea behind localization is we want to construct a ring larger than R that has inverses for the elements in W but changes R as little as possible in every other way.

We will give two constructions. The first was used briefly in a proof from before.

[Hoc17, p. 22] Construction 3.2.1. Let R be a ring, and consider a multiplicative set $W \subseteq R$. Let $R[x_w]_{w\in W}$ be the polynomial ring with possibly infinitely many indeterminates corresponding to elements $w \in W$. Consider the ideal

$$I = (wx_w - 1)_{w\in W} \subseteq R[x_w]_{w\in W}.$$

The composition

$$R \longrightarrow R[x_w]_{w\in W} \twoheadrightarrow \frac{R[x_w]_{w\in W}}{I}$$

turns $R[x_w]_{w\in W}/I$ into an R-algebra with associated structure map denoted by

$$\ell_W \colon R \longrightarrow W^{-1}R.$$

We note that the polynomials in I force the images of the x_w in $W^{-1}R$ to be an inverse for the image of w in $W^{-1}R$, and that $x_{w_1}x_{w_2}\cdots x_{w_n} = x_{w_1w_2\cdots w_n}$ for all $w_1, w_2, \ldots, w_n \in W$, since they both represent inverses of $w_1w_2\cdots w_n$.

We call $W^{-1}R$ the *ring of fractions with respect to* W or the *localization of* R *at* W.

The ring $W^{-1}R$ comes with the following universal property:

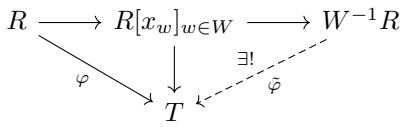
[Hoc17, p. 22] Theorem 3.2.2. *Let R be a ring and consider a multiplicative set $W \subseteq R$. Let $\varphi\colon R \to T$ be a ring map such that $\varphi(w)$ is invertible for every element $w \in W$. Then, there is a unique ring map $\tilde{\varphi}\colon W^{-1}R \to T$ making the diagram*

$$\begin{array}{ccc} R & \xrightarrow{\ell_W} & W^{-1}R \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \exists!\, \tilde{\varphi}} \\ & & T \end{array}$$

commute. In other words, $W^{-1}R$ represents the functor

$$\begin{aligned} \mathsf{Alg}_R &\longrightarrow \mathsf{Sets} \\ T &\longmapsto \big\{ g \in \mathrm{Hom}_R(R, T) \;\big|\; g(w) \text{ is invertible for all } w \in W \big\}. \end{aligned}$$

Proof. We construct the map $\tilde{\varphi}$ from a commutative diagram of the following form:



Note that a map $R[x_w]_{w\in W} \to T$ is uniquely determined by specifying the images of the x_w. We define it by sending x_w to $\varphi(w)^{-1}$, where we note that $\varphi(w)^{-1}$ is uniquely determined by w since multiplicative inverses are unique. This factors uniquely through $W^{-1}R$ as defined above by the universal property for quotient rings (Proposition 1.3.8). □

We now give a second construction. Before we do so, we define the following:

DEFINITION 3.2.3. Let R be a ring. An element $r \in R$ is a *zerodivisor* if $ru = 0$ for some $u \in R - \{0\}$. An element that is not a zerodivisor is called a *nonzerodivisor*, which we abbreviate by *nzd*. [AK21, (2.1)] [Hoc17, p. 22]

The second construction mimics the construction of $\mathbf{Q}$ from $\mathbf{Z}$, but is slightly complicated because there may be zerodivisors in W.

CONSTRUCTION 3.2.4. Let R be a ring, and let $W \subseteq R$ be a multiplicative set. We define an equivalence relation $\sim$ on the product set $R \times W$ as follows:

$(r_1, w_1) \sim (r_2, w_2)$ if and only if there exists $w \in W$ such that $w(r_1w_2 - r_2w_1) = 0$.

Note that if w contains no zerodivisors, then it is the same to require $r_1w_2 - r_2w_1 = 0$. We claim this relation is an equivalence relation.

(1) (Reflexivity) $(r_1, w_1) \sim (r_1, w_1)$ holds since $r_1w_1 - r_1w_1 = 0$.
(2) (Symmetry) $(r_1, w_1) \sim (r_2, w_2)$ if and only if $(r_2, w_2) \sim (r_1, w_1)$ since $w(r_1w_2 - r_2w_1) = -w(r_2w_1 - r_1w_2)$.
(3) (Transitivity) If $(r_1, w_1) \sim (r_2, w_2)$ and $(r_2, w_2) \sim (r_3, w_3)$, then we have two equations:

$$w(r_1w_2 - r_2w_1) = 0 \qquad \text{and} \qquad w'(r_2w_3 - r_3w_2) = 0. \tag{3.2.5}$$

Multiplying the first by $w'w_3$ and the second by ww_1 and adding them together, we obtain

$$ww'w_3(r_1w_2 - r_2w_1) + ww'w_1(r_2w_3 - r_3w_2) = ww'w_2(r_1w_3 - r_3w_1) = 0$$

where $ww'w_2 \in W$ by multiplicativity.

For now, we denote B as the set of equivalence classes in $R \times W$ with respect to this equivalence relation, and denote by r/w the class of (r, w).

The set B is a ring:

- Setting $r_1/w_1 \cdot r_2/w_2 = (r_1r_2)/(w_1w_2)$ is well-defined: If $r_2/w_2 = r_3/w_3$, then we want to show $(r_1r_2)/(w_1w_2) = (r_1r_3)/(w_1w_3)$. By definition of $\sim$, there exists $w \in W$ such that $w(r_2w_3 - r_3w_2) = 0$, in which case
$$w(r_1r_2w_1w_3 - r_1r_3w_1w_2) = r_1w_1 \cdot w(r_2w_3 - r_3w_2) = 0.$$
- Setting $r_1/w_1 + r_2/w_2 = (r_1w_2 + r_2w_1)/(w_1w_2)$ is well-defined: If $r_2/w_2 = r_3/w_3$, then we want to show $(r_1w_2+r_2w_1)/(w_1w_2) = (r_1w_3+r_3w_1)/(w_1w_3)$.

By definition of $\sim$, there exists $w \in W$ such that $w(r_2w_3 - r_3w_2) = 0$, in which case

$$w\big((r_1w_2 + r_2w_1)(w_1w_3) - (r_1w_3 + r_3w_1)(w_1w_2)\big) = w_1^2 \cdot w(r_2w_3 - r_3w_2) = 0.$$

- $0 \in R$ is given by $0/1$, $1 \in R$ is given by $1/1$, and additive inverses are given by $-(r/s) = (-r)/s$.

There ring B is an R-algebra by sending $r \in R$ to $r/1 \in B$. The elements $w/1$ for $w \in W$ are invertible in B, since $w/1 \cdot 1/w = w/w = 1$.

8/30

REMARK 3.2.6. Without the extra w and w' in (3.2.5), we cannot show transitivity: we would have

$$w_3(r_1w_2 - r_2w_1) + w_1(r_2w_3 - r_3w_2) = w_2(r_1w_3 - r_3w_1) = 0,$$

but then we cannot conclude that $r_1w_3 - r_3w_1 = 0$ unless w_2 is a nonzerodivisor.

For a concrete example, consider the localization

$$W^{-1}\left(\frac{k[s,t]}{(st)}\right)$$

where $W = \{1, t, t^2, \ldots\}$. Then, $(s,t) \sim (0,t)$ and $(0,t) \sim (0,1)$ since $st = 0$. However, $(s,t) \not\sim (0,1)$ unless we include the extra w in the definition of $\sim$. In terms of the first construction, we know that $x_t \cdot t = 1$, and hence $0 = x_t \cdot st = s$.

We can show that the two constructions give isomorphic rings.

[Hoc17, p. 23] PROPOSITION 3.2.7. *Let R be a ring, and consider a multiplicative set $W \subseteq R$. Then, Theorem 3.2.2 induces an isomorphism $W^{-1}R \xrightarrow{\sim} B$.*

One can show they are isomorphic by checking that B as constructed above also satisfies the universal property in Theorem 3.2.2; see [AK21, (11.5)] or [AM69, Prop. 3.1]. We give a different proof.

Proof. There is a unique map $W^{-1}R \to B$ by plugging in $T = B$ in Theorem 3.2.2. The map sends x_w to $1/w$ by the description of the map in the proof of Theorem 3.2.2. We claim this is an isomorphism. To do so, we define an inverse by claiming that $R \times W \to W^{-1}R$ where $(r,w) \mapsto rx_w$ is well-defined on equivalence classes: if $(r_1,w_1) \sim (r_2,w_2)$, then their images are $r_1x_{w_1}$ and $r_2x_{w_2}$, respectively, which are the same modulo I since if $w(r_1w_2 - r_2w_1) = 0$, then

$$\begin{aligned} r_1x_{w_1} - r_2x_{w_2} &\equiv wr_1w_2x_{ww_1w_2} - wr_2w_1x_{ww_1w_2} \\ &\equiv x_{w_1w_2} \cdot w(r_1w_2 - r_2w_1) = 0 \end{aligned}$$

where the $\equiv$ denotes equivalence modulo I. These maps define mutually inverse ring maps. □

[Hoc17, pp. 23, 26] LEMMA 3.2.8. *Let R be a ring, and consider a multiplicative set $W \subseteq R$. The kernel of $\ell_W \colon R \to W^{-1}R$ is the ideal*

$$\big\{r \in R \,\big|\, wr = 0 \text{ for some } w \in W\big\}.$$

In particular, $W^{-1}R = 0$ if and only if W contains a nilpotent element.

Proof. An element $r \in R$ maps to zero if and only if $r/1 = 0/1$ in $W^{-1}R$. By definition of the equivalence relation, this holds if and only if $wr = 0$ for some $w \in W$.

The "in particular" statement follows since $1 = 0$ in $W^{-1}R$ if and only if there exists $w \in W$ such that $w \cdot 1 = 0$. □

We give some special cases of this construction.

EXAMPLE 3.2.9. Let R be a ring.

(1) Consider the set S_0 of nonzerodivisors in R. Then, the map $R \to S_0^{-1}R$ is injective, and we call $S_0^{-1}R$ the *total quotient ring* of R. If R is a domain, then $S_0^{-1}R$ is a field, called the *fraction field* of R, which we denote by $\mathrm{Frac}(R)$. For example, applying this construction to $\mathbf{Z}$ gives $\mathbf{Q}$, and applying this construction to $k[x]$ gives the field $k(x)$ of rational functions in x over k. [AK21, (11.3)] [Hoc17, p. 23]

(2) Recall from Proposition 1.4.5 that and ideal $P \subseteq R$ is prime if and only if $R - P$ is a multiplicative set. The localization of R at P is the localization [AK21, (11.21)] [Hoc17, p. 24]

$$R_P \coloneqq (R-P)^{-1}R.$$

The ring R_P is a local ring: every element not in PR_P is a unit by construction. A major theme in commutative algebra will be to reduce questions to questions about local rings by passing to appropriate localizations of the form R_P. [AK21, (11.22)]

(3) Consider an element $f \in R$. The localization of R at $\{1, f, f^2, \ldots\}$ is denoted by R_f. [AK21, (11.12)] [Hoc17, p. 27]

Caution: Do not confuse $\mathbf{Z}_{\langle p \rangle}$ and $\mathbf{Z}_p$! The former inverts all primes not equal to p, while the latter inverts only p.

We prove the analogue of Proposition 1.3.12 for localization to get a geometric interpretation for localization.

PROPOSITION 3.2.10. *Let R be a ring, and let $W \subseteq R$ be a multiplicative set.* [AK21, (11.20)] [Hoc17, pp. 26–27] [AM69, Prop. 3.11]

(*i*) *Every ideal $W^{-1}R$ is of the form $I \cdot W^{-1}R$ for some ideal $I \subseteq R$.*

(*ii*) *There is a bijective inclusion-preserving correspondence*

$$\left\{\begin{matrix}\textit{prime ideals in } R \\ \textit{disjoint from } W\end{matrix}\right\} \longleftrightarrow \left\{\textit{prime ideals in } W^{-1}R\right\}$$

$$P \longmapsto P \cdot W^{-1}R$$

$$\ell_W^{-1}(Q) \longmapsfrom Q$$

Proof. (*i*). Let $J \subseteq W^{-1}R$ be an ideal, and let $I = \ell^{-1}(J)$. We claim $J = I \cdot W^{-1}R$. First, we have $I \cdot W^{-1}R \subseteq J$ by definition, since all elements in I have image in J via $\ell\colon R \to W^{-1}R$. Conversely, suppose $r/w \in J$. Then, $r/1 = w/1 \cdot r/w \in J$, and hence $r \in \ell^{-1}(J) = I$. Since $r \in I$, we see that $r/w \in I \cdot W^{-1}R$.

(*ii*). We first check that the maps have the specified (co)domains in either direction. The map $Q \mapsto \ell^{-1}(Q)$ maps primes to primes, and $\ell^{-1}(Q) \cap W = \emptyset$, for otherwise Q would contain $w \in W$, and hence contain $1 = 1/w \cdot w$. For the other direction, we have

$$\frac{W^{-1}R}{P \cdot W^{-1}R} \simeq \overline{W}^{-1}\frac{R}{P}$$

where $\overline{W}$ denotes the image of W in R/P, since both satisfy the same universal property for ring maps $R \to T$ for which P is killed and the images of elements in W are invertible. Since R/P is a domain, there are two possibilities for the right hand side:

- $0 \in \overline{W}$, in which case the right-hand side is the zero ring.

- We get a subring of the fraction field $\mathrm{Frac}(R/P)$ of R/P, which is a domain.

The two possibilities correspond to when W intersects P and when W is disjoint from P, respectively. □

Next, we want to explain why local rings are called *local* rings.

EXAMPLE 3.2.11. We consider the ring $R = \mathbf{C}[x, y]$ and its localizations. We saw a while ago that $V(f) \subseteq \mathrm{Spec}(R)$ for an irreducible polynomial f contains the prime ideal (f) and all maximal ideals $(x - a, y - b)$ such that $f(a, b) = 0$.

Now let us imagine what $\mathrm{Spec}(R_f)$ should look like. This is the set of prime ideals not containing f, and so should be the complement of $V(f)$, and is an open set.

Now let us imagine what $\mathrm{Spec}(R_{(x-a,y-b)})$ should look like. As a set, this is the intersection

$$\bigcap_{f \notin (x-a,y-b)} \mathrm{Spec}(R_f),$$

which is not open. But it tells us in what way we can interpret $R_{(x-a,y-b)}$ as a local ring: polynomials $g \in R$ that do not vanish at $(x - a, y - b)$ become invertible in $R_{(x-a,y-b)}$, and so $R_{(x-a,y-b)}$ detects whether $g \in R$ is locally invertible at $(x - a, y - b)$.

We use Proposition 3.2.10 to study the twisted cubic again.

EXAMPLE 3.2.12. Consider the twisted cubic curve:

$$\begin{aligned} \varphi\colon k[w, x, y, z] &\longrightarrow k[s, t] \\ w &\longmapsto s^3 \\ x &\longmapsto s^2 t \\ y &\longmapsto s t^2 \\ z &\longmapsto t^3 \end{aligned}$$

We claim that $I = \ker(\varphi)$ cannot be generated by two elements. Suppose that I can be generated by two elements. Then, $J = I \cdot k[w, x, y, z]_{(w,x,y,z)}$ can be generated by two elements. By the NAK Lemma 2.3.8, we know that $wx - xy, xz - y^2, wy - x^2 \in J$ have linearly independent images in $J/(\mathfrak{m} \cdot J)$, where $\mathfrak{m} = (w, x, y, z) \cdot k[w, x, y, z]_{(w,x,y,z)}$.

This is also a good example illustrating the strong connection between graded rings and local rings that you will see on Homework 2!

So while the NAK Lemma 2.3.8 only applies to local rings, it can be useful to study non-local rings as well.

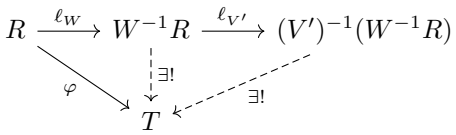
We prove the following:

[AK21, (11.27)] PROPOSITION 3.2.13. *Let R be a ring, and let W be a multiplicative set. Let V' be a multiplicative set in $W^{-1}R$, and set $V = \ell_W^{-1}(V')$. Assume $W \subseteq V$. Then,*

$$(V')^{-1}(W^{-1}R) \simeq V^{-1}R.$$

In particular, if $P \subseteq Q$ are prime ideals, then R_P is the localization of R_Q at $P \cdot R_Q$.

Proof. It suffices to show that $(V')^{-1}(W^{-1}R)$ satisfies the universal property for $V^{-1}R$. Let $\varphi\colon R \to T$ be a ring map such that the elements in $\varphi(V)$ are invertible. We then consider the commutative diagram



The middle dashed arrow exists and is unique since $W \subseteq V$ and by the universal property for ℓ_W. The right dashed arrow exists and is unique by the universal property for $\ell_{V'}$: given an element $v' = v/w \in V'$ where $v \in R$ and $w \in W$, we have $v \in V$ since $w \in W \subseteq V$ has image in V'. This element v/w is therefore invertible in T.

The last statement follows by setting $W = R - Q$ and $V = R_Q - P \cdot R_Q$. □

One can similarly show that if W, V are multiplicative subsets in R, then $(WV)^{-1}R$ is the same as $W^{-1}(V^{-1}R)$ and $V^{-1}(W^{-1}R)$, where these last two rings take the images of W and V in the respective localizations $V^{-1}R$ and $W^{-1}R$, and where WV is the set of products vw, where $v \in V$ and $w \in W$; see [AK21, (11.29)(2)].

3.3. Restriction of scalars

Let R be a ring, let $I \subseteq R$ be an ideal, and consider an R-module M. Then, M/IM has a natural structure as an R/I-module compatible with the R-module structure, by setting

$$(r + I) \cdot (x + IM) = rx + IM$$

for $r \in R$ and $x \in M$. The reason this is well defined is the same as why the R-module structure given by

$$r \cdot (x + IM) = rx + IM$$

is well-defined. These two module structures are connected by the following:

Definition 3.3.1. Let R be a ring, and let S be an R-algebra with structure map $\theta\colon R \to S$. There is then a *restriction of scalars* functor [AK21, (4.5)] [Hoc17, p. 26]

$$\mathsf{Mod}_S \longrightarrow \mathsf{Mod}_R$$

that considers every S-module as an R-module instead by $a \cdot m = \theta(a)m$. Note that this functor is *exact*: it sends exact sequences to exact sequences.

3.4. Localization of modules

We saw in the previous section that there is a way to go from $W^{-1}R$-modules to R-modules. We want to construct a functor that goes in the opposite direction. 9/4

Construction 3.4.1. Let R be a ring, let $W \subseteq R$ be a multiplicative set, and consider an R-module M. We define an equivalence relation $\sim$ on the product set $M \times W$ as follows: [AK21, (12.2)]

$$(m_1, w_1) \sim (m_2, w_2) \text{ if and only if}$$
$$\text{there exists } w \in W \text{ such that } w(m_1 w_2 - m_2 w_1) = 0.$$

As before, this defines an equivalence relation. We denote by $W^{-1}M$ the resulting quotient set, which is a $W^{-1}R$-module by setting $(r/w_1)\cdot(m/w_2) = (rm)/(w_1w_2)$.

This defines a functor.

[AK21, (12.9)] Definition 3.4.2. Let R be a ring, and consider a multiplicative set $W \subseteq R$, and set $S = W^{-1}R$. There is a localization functor

$$\mathsf{Mod}_R \longrightarrow \mathsf{Mod}_{W^{-1}R}$$

sending M to $W^{-1}M$ and $\psi\colon M \to N$ to $W^{-1}\psi\colon W^{-1}M \to W^{-1}N$ by mapping $(W^{-1}\psi)(m/w) = (1/w)\cdot\psi(m)$.

This functor is exact!

[AK21, (12.17)] Proposition 3.4.3. *Let R be a ring and consider a multiplicative set $W \subseteq R$. If $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact, then*

$$W^{-1}M' \xrightarrow{W^{-1}\alpha} W^{-1}M \xrightarrow{W^{-1}\beta} W^{-1}M''$$

is also exact.

Proof. The fact that $\mathrm{im}(W^{-1}\alpha) \subseteq \ker(W^{-1}\beta)$ holds since the composition $\beta\circ\alpha = 0$, and hence the localization $W^{-1}(\beta\circ\alpha) = 0$ as well. It remains to show the reverse inclusion. If $(W^{-1}\beta)(m/w) = 0$, then $\beta(m)/w = 0$, in which case there exists $\tilde{w} \in W$ such that $\tilde{w}\beta(m) = \beta(\tilde{w}m) = 0$. But by exactness, $\tilde{w}m = \alpha(m')$ for some $m' \in M'$, and we see that $m/w = \alpha(m')/(w\tilde{w}) = (W^{-1}\alpha)(m'/(w\tilde{w}))$. □

As a corollary, we can show:

Corollary 3.4.4. *Let R be a ring, and consider a multiplicative set $W \subseteq R$. If $N \subseteq M$ is an inclusion of R-modules, we have*

$$\frac{W^{-1}M}{W^{-1}N} \simeq W^{-1}\left(\frac{M}{N}\right).$$

Proof. Apply Proposition 3.4.3 to the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$ □

Remark 3.4.5. For every ring R and every prime ideal $P \subseteq R$, we have

$$\mathrm{Frac}(R/P) = R_P/PR_P.$$

This is called the *residue field* of R at P. To see this we have

$$\mathrm{Frac}(R/P) = (R/P)_{(0)} \simeq (R/P)_P \simeq R_P/PR_P,$$

where the first equality is by definition, the middle isomorphism is by the fact that the image of $R - P$ in R/P is $(R/P) - (0)$, and the right isomorphism holds by Proposition 3.4.3 and the fact that for every ideal $I \subseteq R$ and every multiplicative [AK21, (11.14)(1)] set $W \subseteq R$, we have

$$W^{-1}I = I \cdot W^{-1}R.$$

The inclusion $\subseteq$ follows from the fact that $i/w = 1/w \cdot i$ for every $i \in I$ and $w \in W$. Conversely, every element in $I \cdot W^{-1}R$ can be written as

$$\sum_{t=1}^{n} i_t \cdot \frac{r_t}{w_t} = \frac{1}{\prod_{t=1}^{n} w_t} \sum_{t=1}^{n} i_t r_t (w_1 \cdots \widehat{w_t} \cdots w_n).$$

3.5. Local properties

We saw that sometimes we can prove statements by passing to localizations. *Local properties* **P** are properties of rings R (resp. modules M) such that R (resp. M) has **P** if and only if R_P (resp. M_P) has **P** for every prime ideal $P \subseteq R$. [AM69, p. 40]

We start with the following fundamental local property: that of being the zero module.

PROPOSITION 3.5.1. *Let R be a ring, and consider an R-module M. The following are equivalent:* [AK21, (13.23)]

(*i*) $M = 0$;
(*ii*) $M_P = 0$ *for every prime ideal* $P \subseteq R$; *and*
(*iii*) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m} \subseteq R$.

Proof. The implications (*i*) $\Rightarrow$ (*ii*) $\Rightarrow$ (*iii*) follow from definition of localization and by the fact that all maximal ideals are prime. We want to show that (*iii*) $\Rightarrow$ (*i*). Let $m \in M$. Since $m/1 = 0 \in M_{\mathfrak{m}}$, there exists $w \in R - \mathfrak{m}$ with $wm = 0$. Thus,

$$\operatorname{Ann}_R(m) \coloneqq \left\{ r \in R \;\middle|\; rm = 0 \right\} \not\subseteq \mathfrak{m}$$

for every maximal ideal $\mathfrak{m}$. We therefore see that $\operatorname{Ann}_R(m) = R$, for otherwise $\operatorname{Ann}_R(m)$ would be contained in a maximal ideal by our application of Zorn's lemma. Thus, $m = 1 \cdot m = 0$. □

We start with one example of a local property of rings.

PROPOSITION 3.5.2. *For every ring R and every multiplicative set $W \subseteq R$, we have* [AK21, (11.18)]

$$\sqrt{(0)}_R \cdot (W^{-1}R) = \sqrt{(0)}_{W^{-1}R}$$

as ideals in $W^{-1}R$, where the radicals are computed in R and $W^{-1}R$, respectively. In particular, the property of being reduced is a local property.

Proof. If an element $f \in R$ is nilpotent, then its image in $W^{-1}R$ is nilpotent, proving $\subseteq$.

Conversely, suppose an element $r/w \in W^{-1}R$ is nilpotent. Then, $(r/w)^n = 0$ for some integer $n > 0$. By the second construction of $W^{-1}R$, there exists $w' \in W$ such that $w'r^n = 0$ in R, and hence $(w'r)^n = 0$ as well. Thus, $w'r$ is nilpotent in R, which shows that $r = 1/w' \cdot w'r \in \sqrt{(0)}_R \cdot (W^{-1}R)$.

The last statement follows from the fact that $\sqrt{(0)} = 0$ if and only if it is zero after localizing at every prime (resp. maximal) ideal. □

COROLLARY 3.5.3. *A map $M \to N$ of R-modules is surjective (resp. injective) if and only if $M_P \to N_P$ is surjective (resp. injective) for every prime ideal $P \subseteq R$ if and only if $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective (resp. injective) for every maximal ideal $\mathfrak{m} \subseteq R$.* [AK21, (13.30)]

Proof. Apply Proposition 3.5.1 to the cokernel (resp. kernel). Note that we are using the exactness of localization (Proposition 3.4.3) here! □

We note the following geometric interpretation of local properties:

DEFINITION 3.5.4. Let R be a ring, and consider an R-module M. The *support* of M is the set [AK21, (13.14)] [Hoc17, p. 98]

$$\operatorname{Supp}(M) \coloneqq \left\{ P \in \operatorname{Spec}(R) \;\middle|\; M_P \neq 0 \right\}.$$

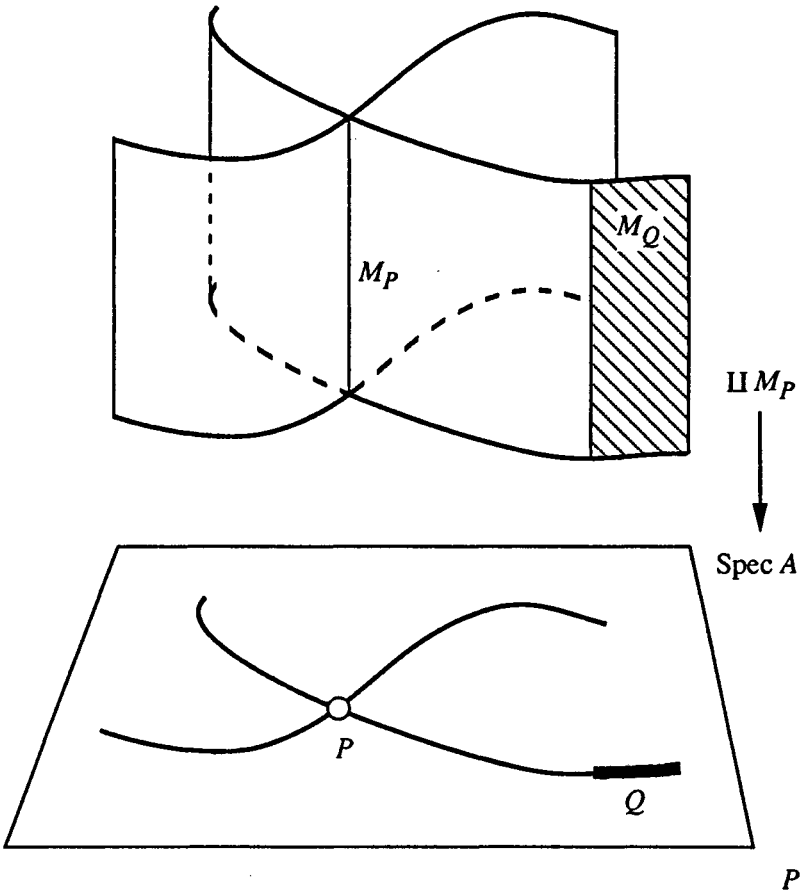


FIGURE 3.1. An A-module M gives rise to the family $\{M_P\}$ of A_P-modules, which we can view as being fibered over $\mathrm{Spec}(A)$. From [Rei95, Figure 7.2].

The way we think of the support geometrically is as follows. We have seen that $\mathrm{Spec}(R)$ is a topological space. We can consider the disjoint union

$$\coprod_{P \in \mathrm{Spec}(R)} M_P \longrightarrow \mathrm{Spec}(R)$$

as a set over $\mathrm{Spec}(R)$, such that all elements in M_P map to $P \in \mathrm{Spec}(R)$. We can draw a picture as in [Rei95, Frontispiece and Figure 7.2], reproduced here as Figure 3.1. This set can be given the structure of a topological space and is a fundamental construction of a sheaf in algebraic geometry. This is an analogue of the notion of a vector bundle in manifold theory. (This space on the left is called an *espace étalé*, which confusingly has nothing to do with étale ring maps. See [God73, Chapitre II, §1.2] or [Har77, Chapter II, Exercise 1.13].)

3.6. More on Spec

Before moving on to the next topic (integral extensions), we want to prove a few more things about $\operatorname{Spec}(R)$ using a bit of what we have learned about localization.

We want to consider the question: *What makes the topological space* $\operatorname{Spec}(R)$ *special?* We start by showing that $\operatorname{Spec}(R)$ is always quasi-compact. Note that what we call a quasi-compact topological space is called *compact* in many texts, for example [Mun00]. The terminology *quasi-compact* is due to Bourbaki [BouGT].

THEOREM 3.6.1. *If R is a ring, then $X = \operatorname{Spec}(R)$ is quasi-compact.* [Hoc17, p. 30]

Proof. Consider an open covering

$$\mathcal{U} = \big\{ X - V(I) \;\big|\; I \in \mathcal{I} \big\},$$

where $\mathcal{I}$ is a family of ideals in R. We have the following sequence of equivalences:

$$\begin{aligned} X = \bigcup_{I\in\mathcal{I}} \big(X - V(I)\big) &\iff \emptyset = \bigcap_{I\in\mathcal{I}} V(I) \\ &\iff \emptyset = V\left(\sum_{I\in\mathcal{I}} I\right) \\ &\overset{1.6.3}{\iff} 1 \in \sum_{I\in\mathcal{I}} I. \end{aligned}$$

Now by definition of the sum of ideals, the last condition holds if and only if there exist a finite subfamily $I_1, I_2, \ldots, I_n$ of ideals in $\mathcal{I}$ and elements $i_j \in I_j$ for each $j \in \{1, 2, \ldots, n\}$ such that $1 = i_1 + i_2 + \cdots + i_n$. Working through the equivalences from above in reverse, we therefore see that

$$X = \bigcup_{j=1}^{n} \big(X - V(I_j)\big)$$

is a finite subcover. □

Recall that sets of the form

$$D(f) \coloneqq \operatorname{Spec}(R) - V(f)$$

are called *principal open sets* (Definition 1.6.2). These form a basis for the Zariski topology since

$$X - V(I) = \bigcup_{a\in I} D(a)$$

for an arbitrary ideal $I \subseteq R$. Moreover, we have $D(a) \cap D(b) = D(ab)$, and hence this basis is closed under finite intersections.

COROLLARY 3.6.2. *The quasi-compact opens in* $\operatorname{Spec}(R)$ *form a basis for the Zariski topology. This basis is stable under finite intersections.* [Hoc17, p. 30]

Proof. Note that $D(a)$ is homeomorphic to $\operatorname{Spec}(R_a)$ by Proposition 3.2.10, and hence are quasi-compact. Since the principal open sets form a basis for the Zariski topology, the quasi-compact open sets form a basis for the Zariski topology as well. Moreover, every quasi-compact open set is a union of principal open sets, and this union can be refined to be a finite union by quasi-compactness. Thus, the intersection of two quasi-compact open sets is also a finite union of principal open sets, and hence is also quasi-compact and open. □

Remark 3.6.3. The property in Corollary 3.6.2 is a topological characterization of when a scheme is *quasi-separated* as defined in algebraic geometry. See [EGAIV$_1$, Proposition 1.2.7].

The next topological property that is very helpful about $\operatorname{Spec}(R)$ is that it is a *sober* space. One way to think of this property is that the space $\operatorname{Spec}(R)$ contains lots of extra points that keep track of closed subsets of $\operatorname{Spec}(R)$ for free. To define this notion, we define irreducibility first.

[Hoc17, p. 30] [Har77, p. 3] [Sha13, p. 34]

Definition 3.6.4. Let X be a topological space. We say that X is *irreducible* if it is nonempty and if, for every pair of proper closed subsets $X_1, X_2 \subsetneq X$, we have $X_1 \cup X_2 \subsetneq X$. Otherwise, we say that X is *reducible*.

When we say a subset $Y \subseteq X$ is irreducible, we will mean that Y is irreducible with the subspace topology.

Remark 3.6.5 (Why the empty set is reducible). The condition that X is nonempty is part of Definition 3.6.4. Following [BouCA, p. 94], one can alternatively define X to be irreducible if for every finite collection of proper closed subsets $X_i \subsetneq X$, we have $\bigcup_i X_i \subsetneq X$. The empty set is reducible under this definition by using the empty collection of proper closed subsets in $\emptyset$.

Definition 3.6.6 [EGAI$_{\text{new}}$, Chapitre 0, (2.1.1)]. A topological space X is *sober* if every closed irreducible subset $Z \subseteq X$ admits a *generic point*, that is, a point $z \in Z$ such that $\overline{\{z\}} = Z$.

[Hoc17, p. 13]

Remark 3.6.7. For a ring R, the space $\operatorname{Spec}(R)$ is T_0: If P and Q are distinct primes, there exists an element $u \in P - Q$ (or $u \in Q - P$), and $V(u) \ni P$ but $V(u) \not\ni Q$ (or vice versa). For T_0 spaces, generic points (if they exist) are unique.

What algebraic property corresponds to irreducibility? For domains, we know that (0) is the unique prime ideal contained in all other prime ideals. How far can we go from being a domain? By the Scheinnullstellensatz (Theorem 1.5.7), the topology of $\operatorname{Spec}(R)$ does not change if we kill the nilradical $\sqrt{(0)}$. The next proposition says that this is the only difference that can occur.

Proposition 3.6.8. *Let R be a ring.*

(*i*) $\operatorname{Spec}(R)$ *is irreducible if and only if the nilradical $\sqrt{(0)}$ is prime. In this case, $\sqrt{(0)}$ is the unique minimal prime ideal of R and corresponds to a generic point for* $\operatorname{Spec}(R)$.

(*ii*) *R is a domain if and only if it is reduced and* $\operatorname{Spec}(R)$ *is irreducible.*

(*iii*) *In* $\operatorname{Spec}(R)$*, the closed subset $V(I)$ is irreducible if and only if $P = \sqrt{I}$ is prime. In this case, P is a generic point for $V(I) = V(P)$.*

Proof. It suffices to show only one of (*i*) and (*ii*) since as mentioned above, the topology of $\operatorname{Spec}(R)$ does not change if we kill the nilradical $\sqrt{(0)}$ by the Scheinnullstellensatz (Theorem 1.5.7). Moreover, (*iii*) follows from either (*i*) or (*ii*) by applying (*i*) or (*ii*) to R/I.

We will show (*ii*). If R is a domain, then (0) is the unique minimal prime ideal of R. For the converse, we prove the contrapositive. Suppose that R is not a domain. Consider two nonzero elements $a, b \in R$ such that $ab = 0$. Then, every prime ideal in R must contain a or b, and hence

$$\operatorname{Spec}(R) = V(a) \cup V(b).$$

If both $V(a)$ and $V(b)$ are proper closed subsets, then $\mathrm{Spec}(R)$ is reducible. If one of $V(a)$ or $V(b)$ equals $\mathrm{Spec}(R)$, then in each respective situation, we have $a \in \sqrt{(0)}$ and $b \in \sqrt{(0)}$. □

The following miraculous theorem says that the properties of $\mathrm{Spec}(R)$ that we have proved so far *exactly* characterize which topological spaces can be constructed as the spectrum of a ring. This result is one of the main results in Hochster's thesis (published as [Hoc69]). The class of topological spaces appearing in Hochster's theorem are called *spectral spaces* and appear in many contexts. For example, the point set topology of spectral spaces is fundamental in the theory of diamonds (the analogue of algebraic spaces for perfectoid spaces) [Sch22].

THEOREM 3.6.9 [Hoc69, Theorem 6]. *Let X be a topological space. There exists a ring R such that X is homeomorphic to* $\mathrm{Spec}(R)$ *if and only if X is a sober quasi-compact T_0 space in which the quasi-compact open sets are stable under finite intersections and form a basis for the topology on X.* [Hoc17, p. 31]

3.6.1. The universal property of polynomial rings. One thing we did not cover before is that polynomial rings have the following universal property. 9/6

PROPOSITION 3.6.10. *Let R be a ring and let $\{x_i\}_{i\in I}$ be a set of variables. Given a ring map $\varphi\colon R \to S$ and a set of elements $s_i \in S$, there is a unique map $\pi\colon R[\{x_i\}_{i\in I}] \to S$ such that $\pi(x_i) = s_i$ for every i and such that the diagram* [AK21, (1.3)]

$$\begin{array}{ccc} R & \longrightarrow & R\big[\{x_i\}_{i\in I}\big] \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \exists!\,\pi} \\ & & S \end{array}$$

commutes.

In other words, $R[x_1, x_2, \ldots, x_n]$ represents the functor that sends an R-algebra S to subsets of n elements in S, or "mapping from $R[x_1, x_2, \ldots, x_n]$ to S is the same as choosing n elements in S."

Proof. The map π is a ring map by the definition of addition and multiplication of polynomials. It is unique since the polynomial ring is generated by the x_i and 1 as an R-algebra. □

CHAPTER 4

Integral extensions

The next segment of this course will focus on studying integral extensions of rings and dimension of rings. The fundamental definitions and results for rings (as opposed to Dedekind domains) is due to Noether [Noe27]. The Incomparability, Lying over, Going up, and Going down theorems are due to Krull [Kru37] (for integral domains) and to Cohen and Seidenberg [CS46] (in general).

4.1. Motivation: How can we tell rings apart?

We have been playing with a few examples so far, but we have not talked too much about how we know they are different. For example:

EXAMPLE 4.1.1. The integers $\mathbf{Z}$ and the polynomial ring $k[x]$ have similar looking spectra, but are not isomorphic since one contains a field, and the other does not.

Another way in which $\mathbf{Z}$ and $k[x]$ are similar is that they are PID's, and both are of dimension 1. Now is a good time to define dimension:

DEFINITION 4.1.2. Let R be a ring, and let [Hoc17, p. 32] [AK21, (15.9)]

$$P_0 \subsetneq P_1 \subsetneq \cdots \subseteq P_d$$

be a chain of prime ideals with strict inclusions. The *Krull dimension* $\dim(R)$ of R is the supremum of lengths of finite strictly increasing chains of prime ideals in $\operatorname{Spec}(R)$, and may be $+\infty$. The dimension of the zero ring is -1 by convention.

EXAMPLE 4.1.3. The rings $\mathbf{Z}$ and $\mathbf{Z}[x]$ are not isomorphic (resp. k, $k[x]$, and $k[x,y]$ are not isomorphic): they have maximal chains of prime ideals of different length. Fields have dimension zero, PID's that are not fields have dimension one.

This gives a first, coarse way to tell rings apart. But there are some difficult questions we do not know the answer to:

EXAMPLE 4.1.4. Let R and S be rings. Then, $R[x] \simeq S[y]$. Is the converse true? [Hoc17, pp. 29–30] This is false: Hochster found an example in 1972 [Hoc72a] and Danielewski gave a simple example in 1989 [Dan89]: [Des66, p. 306]

$$R = \frac{\mathbf{C}[x,y,z]}{(xy-(1-z^2))} \qquad \text{and} \qquad S = \frac{\mathbf{C}[x,y,z]}{(x^2y-(1-z^2))}.$$

On the other hand, if we specialize to the case where R is the polynomial ring $k[t_1,t_2,\ldots,t_n]$ over a field, then there are some open problems.

(1) The $n=1$ case is true: this is a theorem of Abhyankar, Eakin, and Heinzer [AEH72].

(2) The $n = 2$ case is true: in characteristic zero, this is a theorem of Fujita [Fuj79] and Miyanishi and Sugie [MS80], and in positive characteristic, it is due to Russell [Rus81] when k is perfect and Bhatwadekar and Gupta [BG15] in general.
(3) The $n \geq 3$ case was shown to be false in positive characteristic by Gupta in 2014 [Gup14a; Gup14b], but is open in characteristic zero.

We won't be so ambitious! For now, we want to introduce one example where thinking about integral extensions allows us to distinguish two rings that look pretty similar.

EXAMPLE 4.1.5 (The cuspidal cubic). Let k be a field and consider the ring $k[t^2, t^3] \subseteq k[t]$. Both these rings are dimension 1 (we do not yet have the tools to show this, but it is true), and their fraction fields are both $k(t)$. However, note that

$$t \in \operatorname{Frac}\big(k[t^2, t^3]\big)$$

is an element that satisfies a monic polynomial with coefficients in $k[t^2, t^3]$, namely $X^2 - t^2$. The ring $k[t]$ does not have this property: Suppose $f/g \in \operatorname{Frac}(k[t])$ is a rational function with $\gcd(f, g) = 1$ that satisfies a monic polynomial

$$X^d + r_{d-1}X^{d-1} + \cdots + r_0 \cdot 1$$

with coefficients in $k[t]$. Then, we have

$$f^d = -r_{d-1}f^{d-1}g - \cdots - r_0 g^d,$$

and hence a factor of g divides f, a contradiction. Thus, $k[t^2, t^3]$ and $k[t]$ are not isomorphic. (Note: What we have used here is that $k[t]$ is a UFD. For these two rings, another way to distinguish them is to see that $(t^2)^3 = (t^3)^2$ gives two factorizations of t^6, and hence $k[t^2, t^3]$ is not a UFD.)

In this example, t is an element of $k(t)$ (or even $k[t]$) that is *integral* over $k[t^2, t^3]$.

4.2. Integral extensions

The main technical idea we will use is that of integral extensions, which are the ring-theoretic analogue of algebraic field extensions. We will use this theory to prove some fundamental results like Hilbert's Nullstellensatz.

[Hoc17, p. 33]
[AK21, (10.21)]

DEFINITION 4.2.1. Let R be a ring, and let S be an R-algebra. An element $s \in S$ is *integral* over R if for some positive integer d we have that

$$s^d = r_{d-1}s^{d-1} + \cdots + r_1 s + r_0 \cdot 1_S \tag{4.2.2}$$

for suitable elements $r_j \in R$.

[Hoc17, p. 35]
[AK21, (10.23)]

LEMMA 4.2.3. *Let R be a ring, and let S be an R-algebra with structure map $\theta\colon R \to S$. For an element $s \in S$, the following are equivalent:*

(*i*) *s is integral over R.*
(*ii*) *The R-submodule of S spanned by the powers of s is finitely generated as a module over R.*
(*iii*) *s is integral over the image $\theta(R)$ of R in S.*
(*iv*) *The $\theta(R)$-submodule of S spanned by the powers of s is finitely generated as a module over $\theta(R)$.*

Proof. For (*i*) ⇒ (*ii*), we claim that $s^{d-1}, \dots, 1_S$ generate the R-submodule S' of S spanned by the powers of s. We show that s^t is in S' by induction on $t \geq 0$. The case $t \leq d-1$ is true by definition of this submodule, and the $t = d$ case follows by definition of integrality, since $s^d \in Rs^{d-1} + \cdots + R1_S$. Now suppose that s^{t-1} is in this module; we want to show that s is. Then, we can write

$$\begin{aligned} s^t &= s(s^{t-1}) \\ &= s(x_{d-1}s^{d-1} + \cdots + x_1 s + x_0 \cdot 1_S) \\ &= x_{d-1}s^d + x_{d-2}s^{d-1} + \cdots + x_1 s^2 + x_0 s \\ &= x_{d-1}(r_{d-1}s^{d-1} + \cdots + r_1 s + r_0 \cdot 1_S) + x_{d-2}s^{d-1} + \cdots + x_1 s^2 + x_0 s. \end{aligned}$$

For (*ii*) ⇒ (*i*), it suffices to note that if $s^{d-1}, \dots, 1_S$ generate S' as an R-module, then s^d must be an R-linear combination of $s^{d-1}, \dots, 1_S$. This yields an equation of the form (4.2.2).

For the other two equivalent statements, note that $R \to \theta(R)$ is surjective, and hence (4.2.2) holds for $r_i \in R$ if and only if it holds for some $a_i \in \theta(R)$. □

Example 4.2.4. Consider the extension $\mathbf{Z} \subseteq \mathbf{Q}$. The element $1/2$ is not integral over $\mathbf{Z}$: none of its dth powers are $\mathbf{Z}$-linear combinations of lower powers of $1/2$.

Now consider the extension $\mathbf{Z} \subseteq \mathbf{Z}[\sqrt{2}]$. The element $\sqrt{2}$ is integral over $\mathbf{Z}$: $\sqrt{2}$ satisfies the monic polynomial $x^2 - 2 = 0$.

Definition 4.2.5. We say that an R-algebra S is *integral* over R or that the structure map $\theta\colon R \to S$ is *integral* if every element of S is integral over R. If $\theta\colon R \subseteq S$ is an injective ring map and S is integral over R, then we say that S is an *integral extension* of R. To reduce ambiguity, we say that S is *module-finite* over R or that $\theta\colon R \to S$ is *module-finite* if S is finitely generated as a module over R. If $R \subseteq S$ is an extension and S is module-finite over R, we call this a *module-finite extension*.

[Hoc17, pp. 33–34] [AK21, (10.21)]

To reduce ambiguity, if S is finitely generated as an R-algebra, we sometimes say that S is of *finite type* or that $\theta\colon R \to S$ is of *finite type*.

Our first goal for today is to prove:

Theorem 4.2.6. *Let R be a ring, and let S be an R-algebra. Then, S is integral and is finitely generated as an algebra over R if and only if S is module-finite over R.*

[AK21, (10.28)] [Hoc17, p. 37]

The main trick is to use linear algebra. The following result is a version of the Cayley–Hamilton theorem for modules. Below, we denote by $\mathrm{End}_R(M)$ the R-module $\mathrm{Hom}_R(M, M)$, which is a non-commutative ring.

Note that while $\mathrm{End}_R(M)$ is non-commutative, the ring $R[\varphi]$ that appears in the proof below is commutative. See [Hoc17, p. 34] or [HK71, Chapter 5] for treatments of the theory of determinants over arbitrary commutative rings.

Theorem 4.2.7 (Determinant trick). *Let R be a ring, and consider a finitely generated R-module M. Let $\varphi\colon M \to M$ be an R-module map. Then, φ satisfies a monic relation*

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

in $\mathrm{Hom}_R(M, M)$, where $a_i \in R$ for every i. If also $\varphi(M) \subseteq IM$ for some ideal $I \subseteq R$, then $a_i \in I^i$ for every i.

[AK21, (10.2)] [Rei95, (2.7)] [Hoc17, pp. 34–35] [AM69, Prop. 2.4]

Proof. Let $m_1, m_2, \dots, m_n$ be a set of generators for M. Write $\varphi(m_i) = \sum_j a_{ij} m_j$ for $a_{ij} \in R$ (or in I in the second case). Consider the $(n \times n)$-matrix

$$A = (a_{ij})_{1 \le i,j \le n}.$$

We then obtain

$$A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = (a_{ij}) \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} \varphi(m_1) \\ \varphi(m_2) \\ \vdots \\ \varphi(m_n) \end{pmatrix} = \varphi \cdot \mathrm{id} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$$

and hence

$$(A - \varphi \cdot \mathrm{id}) \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

where $A - \varphi \cdot \mathrm{id}$ is a matrix with entries in $R[\varphi] \subseteq \mathrm{End}_R(M)$. Multiplying on the left by the adjugate matrix $\mathrm{adj}(A - \varphi \cdot \mathrm{id})$ (or the classical adjoint matrix, whose (i,j)-th entry is the (j,i)-th cofactor of A), we obtain

$$\det(A - \varphi \cdot \mathrm{id}) \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

This implies that

$$\pm \det(A - \varphi \cdot \mathrm{id})(m_i) = 0$$

for every i, and hence

$$\pm \det(A - \varphi \cdot \mathrm{id}) = 0$$

in $\mathrm{End}_R(M)$, which is an expression of the form we want. □

We can now prove one direction of Theorem 4.2.6.

Proof of $\Leftarrow$ in Theorem 4.2.6. Suppose $R \to S$ is module-finite. As we discussed in Example 3.1.2, module-finite algebras are also finitely generated as algebras. Now for every $s \in S$, we see that the multiplication by s map $\varphi_s \in \mathrm{End}_R(S)$ satisfies

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

by Theorem 4.2.7. Now applying this equation to $1_S \in S$, we obtain

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

and hence every $s \in S$ is integral over R. □

To prove the other direction in Theorem 4.2.6, we will use the following:

[Hoc17, p. 36]
[AK21, (10.26), (10.27)]

LEMMA 4.2.8. *Let*

$$R \xrightarrow{\alpha} S \xrightarrow{\beta} T$$

be a sequence of ring maps. If α and β are integral (resp. module-finite), then so is $\beta \circ \alpha$.

Proof. We first prove the statement for module-finiteness: if $t_1, t_2, \ldots, t_n$ generate T over S and if $s_1, s_2, \ldots, s_m$ generate S over R, then the set

$$\left\{ s_i t_j \;\middle|\; 0 \leq i \leq m,\ 0 \leq j \leq n \right\}$$

is a set of generators for T over R, since any element in T can be written as

$$\sum_{j=1}^{n} \sigma_j t_j = \sum_{j=1}^{n} \sum_{i=1}^{m} r_{ij} s_i t_j,$$

where $\sigma_j \in S$ and $r_{ij} \in R$.

Now consider the integrality statement. Let $t \in T$ be integral over S, and consider a monic relation

$$t^d + s_1 t^{d-1} + \cdots + s_d = 0.$$

For each $j \leq d$, consider the ring maps

$$R \longrightarrow R[s_1] \longrightarrow R[s_1, s_2] \longrightarrow \cdots \longrightarrow R[s_1, s_2, \ldots, s_d] \longrightarrow R[s_1, s_2, \ldots, s_d, t].$$

By Lemma 4.2.3, each ring map is module-finite, and by the module-finite case of this lemma, the ring $R[s_1, s_2, \ldots, s_d, t]$ is module-finite over R. Thus, t is integral over R by the implication $\Leftarrow$ in Theorem 4.2.6. □

We can now prove the remaining implication in Theorem 4.2.6.

Proof of $\Rightarrow$ in Theorem 4.2.6. Suppose S is integral and finitely generated as an algebra over R. Let $s_1, s_2, \ldots, s_m$ be a set of generators for S as an R-algebra. Then, we consider a sequence

$$R \longrightarrow R[s_1] \longrightarrow R[s_1, s_2] \longrightarrow \cdots \longrightarrow R[s_1, s_2, \ldots, s_m]$$

as before. Since each map is module-finite by Lemma 4.2.3, the composition is module-finite by Lemma 4.2.8. □

As a consequence, given a ring map $R \to S$, the set of elements in S integral over R forms a subring. 9/9

Definition 4.2.9. Let R be a ring, and let S be an R-algebra. The *integral closure* of R in S is the subset $\overline{R} \subseteq S$ of elements integral over R. [Hoc17, p. 36] [AK21, (10.19)]

Corollary 4.2.10. *Let R be a ring, and let S be an R-algebra with structure map $\theta\colon R \to S$. Then, the integral closure $\overline{R} \subseteq S$ is a subring in S, and is integrally closed in S.* [Hoc17, p. 36] [AK21, (10.32)]

Proof. Let $s_1, s_2 \in S$ be integral over R. In the commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & \theta(R)[s_1, s_2] \\ & \searrow \quad \nearrow & \\ & \theta(R)[s_1] & \end{array}$$

the two diagonal arrows are module-finite, and hence their composition is module-finite by Lemma 4.2.8. Thus, the R-subalgebra $\theta(R)[s_1, s_2]$ consists of elements integral over R by Theorem 4.2.6. The last statement follows from Lemma 4.2.8. □

REMARK 4.2.11. Actually writing down the integral polynomial satified by $s_1 s_2$ is difficult. One can show that if s_1 satisfies a monic polynomial of degree d_1 and s_2 satisfies a monic polynomial of degree d_2, then $s_1 s_2$ satisfies a monic polynomial of degree $d_1 d_2$. See [Her75, Corollary to Theorem 5.1.4], which states the analogous result for algebraic field extensions. An algebraic field extension is the special case of an integral ring extension when both rings are fields. The proof in [Her75] reduces to the case of finite field extensions in a similar way to how we reduced to the case of a module-finite ring extension.

To explicitly write down the monic polynomial satisfied by $s_1 s_2$, one can use the theory of resultants (see, e.g., [Jac85, Theorem 5.7]). If s_1 satisfies a monic polynomial f_1 and s_2 satisfies a monic polynomial f_2, then $s_1 + s_2$ satisfies the monic polynomial $\operatorname{Res}(f_1(x), f_2(z-x))$ in z and $s_1 s_2$ satisfies the monic polynomial $\operatorname{Res}(f_1(x), x^{\deg(f_2)} f_2(z/x))$ in z.

[Hoc17, p. 43] [AK21, (10.19)] DEFINITION 4.2.12. Let R be a ring, and let S be an R-algebra. If R is reduced (resp. if R is a domain), we call the integral closure $\overline{R}$ in the total quotient ring (resp. fraction field) of R the *normalization* or *integral closure* of R. We say that R is *integrally closed* or *normal* if $R = \overline{R}$.

[AK21, (10.34)] EXAMPLE 4.2.13. We give some examples of rings and their normalizations.

[AK21, (10.33)] (1) (Gauss) A UFD is normal. In particular, polynomial rings over fields or PID's are normal.

Proof. Let R be a UFD, and consider $r/s \in \operatorname{Frac}(R)$, where r and s are relatively prime. Now consider a monic relation

$$\left(\frac{r}{s}\right)^n = a_1\left(\frac{r}{s}\right)^{n-1} + \cdots + a_n.$$

Clearing denominators, we get a relation

$$r^n = s(a_1 r^{n-1} + a_2 r^{n-2} s + \cdots + a_n s^{n-1}).$$

Since R is a UFD, any prime element dividing s also divides r, and hence s is a unit. Thus, $r/s \in R$. □

The next class of examples are rings of integers or things like them.

[Hoc17, p. 36] (2) Let $\mathbf{Q} \subseteq F$ be a finite algebraic field extension. Then, the integral closure $\mathcal{O}$ of $\mathbf{Z}$ in F is the ring of algebraic integers of F. These are the fundamental objects in algebraic number theory.

(3) The ring $R = \mathbf{Z}[\sqrt{5}]$ is not a UFD since

$$(1+\sqrt{5})(1-\sqrt{5}) = -4 = -2 \cdot 2,$$

and $1+\sqrt{5}$, $1-\sqrt{5}$, and 2 are irreducible but are not multiples of each other by a unit. The ring R is also not normal, since the golden ratio

$$\tau := \frac{1+\sqrt{5}}{2}$$

satisfies the monic relation $\tau^2 - \tau - 1 = 0$. The ring $\mathbf{Z}[\tau]$ is therefore contained in the normalization $\overline{R}$ of R. We claim that $\mathbf{Z}[\tau]$ is the normalization of R. We can see this since $\mathbf{Z}[\tau]$ is a Euclidean domain with gauge function

$$a + b\tau \longmapsto |a^2 + ab - b^2|,$$

[Hoc17, p. 43–44] and hence is a UFD (even a PID). Alternatively, we can proeed in an

elementary way as follows: If $a+b\sqrt{5}$ is integral over $\mathbf{Z}[\sqrt{5}]$ with $a, b \in \mathbf{Q}$, then $a-b\sqrt{5}$ satisfies the same monic polynomial over $\mathbf{Z}$ that $a+b\sqrt{5}$ does, and is therefore integral over $\mathbf{Z}$. Their sum $2a$ is therefore also integral over $\mathbf{Z}$, in which case $a = k$ or $k+1/2$ for some integer k. By subtracting a suitable integer linear combination of $\sqrt{5}$ and τ from $a+b\sqrt{5}$, we have an element of the form $c\sqrt{5}$ that is integral over $\mathbf{Z}$, such that $c \in \mathbf{Q}$. It will therefore suffice to show that if c is rational and $c\sqrt{5}$ is integral over $\mathbf{Z}$, then c is an integer. Write $c = m/n$ where m and n are coprime. Then, $5c^2$ is rational and integral over $\mathbf{Z}$, and is therefore an integer, i.e., $n^2 \mid 5m^2$. By prime factorization, we see that $5 \nmid n$. Then, $n^2 \mid m^2$, and hence c is a rational number whose square is an integer. It follows that c itself is an integer.

(4) Let $d \in \mathbf{Z}$ be square-free. In $K \coloneqq \mathbf{Q}(\sqrt{d})$, form the ring $R \coloneqq \mathbf{Z} + \mathbf{Z}\delta$, where

$$\delta \coloneqq \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4; \\ \sqrt{d} & \text{if } d \not\equiv 1 \bmod 4. \end{cases}$$

Then, R is the normalization $\overline{\mathbf{Z}}$ of $\mathbf{Z}$ in K.

(5) The ring $\mathbf{Z}[\sqrt{p}]_{p \geq 2 \text{ prime}}$ is integral over $\mathbf{Z}$ but is not module-finite nor finitely generated as an algebra over $\mathbf{Z}$, since adjoining square roots of finitely many primes cannot introduce square roots for other primes. Similarly, $k[x^{1/2^n}]_{n \geq 1}$ is integral over $k[x]$ but is not module-finite nor finitely generated as an algebra over $k[x]$. [Hoc17, p. 37]

Now we consider some geometric examples.

(6) Let k be a field, and consider the subring $R = k[t^2, t^3] \subseteq k[t]$. Since $t = t^3/t^2 \in \mathrm{Frac}(R)$, we see that $\mathrm{Frac}(R) = k(t)$. Now note that $t \in \mathrm{Frac}(R)$ satisfies $z^2 - t^2 = 0$, and hence $t \in \overline{R}$. But since $k[t]$ is already normal, we see that the normalization of R is $k[t]$.

Being normal is a local property. We first show that the property that a ring map is integral is a local property.

Proposition 4.2.14. *Let $R \to S$ be a ring map, and let $W \subseteq R$ be a multiplicative set. Then, $W^{-1}\overline{R} = \overline{W^{-1}R}$ as subrings of $W^{-1}S$.* [AK21, (11.32)] [AM69, Prop. 5.12]

Proof. We first show $\subseteq$. Given $r/w \in W^{-1}\overline{R}$, we know that r satisfies a monic relation

$$r^n = a_1 r^{n-1} + a_2 r^{n-2} + \cdots + a_n.$$

Now dividing throughout by w^n, we obtain

$$\left(\frac{r}{w}\right)^n = \frac{a_1}{w}\left(\frac{r}{w}\right)^{n-1} + \frac{a_2}{w^2}\left(\frac{r}{w}\right)^{n-2} + \cdots + \frac{a_n}{w^n},$$

and hence $r/w \in \overline{W^{-1}R}$. Conversely, if $r/w \in \overline{W^{-1}R}$, we have an equation of the form

$$\left(\frac{r}{w}\right)^n = \frac{a_1}{w_1}\left(\frac{r}{w}\right)^{n-1} + \frac{a_2}{w_2}\left(\frac{r}{w}\right)^{n-2} + \cdots + \frac{a_n}{w_n}.$$

Clearing denominators by multiplying by $(ww_1w_2\cdots w_n)^n$, we obtain a monic relation for $r(w_1w_2\cdots w_n)$ over R, and hence $r/w \in W^{-1}\overline{R}$. □

Corollary 4.2.15. *Let R be a domain. Then, the following are equivalent:* [AM69, Prop. 5.13]

(*i*) *R is normal.*
(*ii*) *R_P is normal for every prime ideal $P \subseteq R$.*
(*iii*) *$R_{\mathfrak{m}}$ is normal for every maximal ideal $\mathfrak{m} \subseteq R$.*

Proof. Consider the ring extension $R \to \overline{R}$. This map is surjective if and only if it is surjective after localizing at every P (resp. every $\mathfrak{m}$). Now the claim follows by the fact that normalization is compatible with localization (Proposition 4.2.14). □

4.3. Lying over and incomparability

We will now focus on proving some fundamental results about integral extensions, called the Cohen–Seidenberg theorems [CS46] (although as we noted before, they are due to Krull [Kru37] for integral domains). We start with the following:

[Hoc17, p. 38] LEMMA 4.3.1. *Let $R \subseteq S$ be an integral extension of rings, let $I \subseteq R$ be an ideal, and consider $u \in IS$. Then, u satisfies a monic polynomial equation*

$$u^n + a_1 u^{n-1} + \cdots + a_{n-1}u + a_n = 0,$$

where $a_i \in I^i$ for every i.

Proof. We want to use the determinant trick (Theorem 4.2.7). Since u is integral over R, we can write

$$u = \sum_{i=1}^{n} s_i a_i$$

for $s_i \in S$ and $a_i \in I$. Replacing S by the subring generated by u and the s_i, we may assume that S is module-finite over R.

Now consider the R-module map

$$\varphi_u \colon S \longrightarrow S.$$

Since $u \in IS$, we see that $\varphi_u(S) \subseteq IS$ by definition. We therefore see that

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

by the determinant trick (Theorem 4.2.7), and evaluating at 1_S gives the desired polynomial equation. □

REMARK 4.3.2. Lemma 4.3.1 suggests why the integral closure of an ideal is defined in the way it is [SH06, Definition 1.1.1]. The definition of integral closure for ideals is also due to Krull [Kru36]. Note that the definition of the integral closure of an ideal in [AM69, p. 63] is not the standard definition!

We can now show:

[Hoc17, p. 38] THEOREM 4.3.3. *Let $R \subseteq S$ be an integral extension of rings.*

[McQ79, Rem. 3] (*i*) *For every ideal $I \subseteq R$, we have $IS \cap R \subseteq \sqrt{I}$. Thus, if I is radical, then $IS \cap R = I$.*

[AK21, (14.3)(3)] (*ii*) *(Lying over) Consider a prime ideal $P \subseteq R$. There exists a prime $Q \subseteq S$ such that $Q \cap R = P$. In other words, $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is surjective.*

This version of Lying over is [CS46, Theorem 2].

Proof. We first show (*i*). Let $u \in IS \cap R$. By Lemma 4.3.1, the element u satisfies a monic equation

$$u^n = -(a_1 u^{n-1} + \cdots + a_{n-1}u + a_n) \in I,$$

since $a_i \in I^i$ for every i.

We now show (*ii*). Let P be a prime ideal. Then, $R - P$ is a multiplicative set in R, and hence is a multiplicative set in S. By (*i*), $PS \cap R = P$, and hence $R - P$ is disjoint from PS. By one of our applications of Zorn's lemma (Proposition 1.5.5), there exists a prime ideal $Q \subseteq S$ that contains PS but is disjoint from $R - P$. Since $P \subseteq PS$, we see that

$$P = PS \cap R \subseteq Q \cap R = (Q \cap P) \cup (Q \cap R - P) \subseteq P. \qquad \square$$

We next investigate whether there can be two primes lying over the same prime in R.

THEOREM 4.3.4. *Let $R \subseteq S$ be an integral extension of rings.*

(*i*) *Suppose R and S are domains. Then, every element $s \in S - \{0\}$ has a nonzero multiple in R.* [Hoc17, p. 37]

(*ii*) *(Incomparability) Consider a prime ideal $P \subseteq R$. If Q_1 and Q_2 are two prime ideals in S such that $Q_1 \cap R = P = Q_2 \cap R$, then $Q_1 \not\subseteq Q_2$ and $Q_2 \not\subseteq Q_1$.* [AK21, (14.3)(2)] [Hoc17, p. 38]

This version of Incomparability is [CS46, Theorem 4].

Proof. We first prove (*i*). Consider an equation of integral dependence

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

where $a_i \in R$ for all i. Since $s \neq 0$, one of the a_i must be nonzero. Now if h is the smallest i such that $a_h \neq 0$, then we can rewrite the equation as

$$s^h(s^{n-h} + \cdots + a_{h+1}s + a_h) = 0.$$

Since $s \neq 0$ and S is a domain, $s^{n-h} + \cdots + a_{h+1}s + a_h = 0$, and hence

$$0 \neq a_h = -s(s^{n-h-1} + \cdots + a_{h+1}) \in R.$$

Finally, we show (*ii*). Let Q_1 be a prime ideal lying over P. It suffices to show that every prime ideal $Q_2 \supsetneq Q_1$ cannot lie over P. The extension $R/P \subseteq S/Q_1$ is still integral, since every $\bar{s} \in S/Q_1$ lifts to an element $s \in S$ satisfying a monic polynomial over R. Now since $Q_2 \supsetneq Q_1$, there exists a nonzero element $u \in Q_2(S/Q_1)$. By (*i*), u has a nonzero multiple in R/P, and hence $Q_2(S/Q_1) \cap (R/P) \neq (0)$. $\square$

We give another proof of Lying Over that does not use the determinant trick. This proof illustrates how useful and powerful reductions are. 9/11 [Hoc17, p. 39]

THEOREM 4.3.5 (Lying over). *Let $R \subseteq S$ be an integral extension of rings. Consider a prime ideal $P \subseteq R$. There exists a prime $Q \subseteq S$ such that $Q \cap R = P$.*

We first note the following:

LEMMA 4.3.6. *Let $R \subseteq S$ be an integral extension of rings. Let $W \subseteq R$ be a multiplicative set. Then, $W^{-1}R \to W^{-1}S$ is an integral extension.* [Hoc17, p. 39]

Proof. The proof is very similar to the proof of Proposition 4.2.14. The map $W^{-1}R \to W^{-1}S$ is injective by the exactness of localization (Proposition 3.4.3). The extension is integral since $W^{-1}S$ is generated by the elements $s/1$, which satisfy monic polynomials over the image of $R \to W^{-1}R$. □

We now give our second proof of Lying Over.

Proof of Theorem 4.3.5. We first reduce to the case when R is local with maximal ideal P. We apply Lemma 4.3.6 with $W = R - P$. Let $S_1 = W^{-1}S$. If $Q_1 \subseteq S_1$ is a prime ideal lying over PR_P, then the contraction Q of Q_1 to S will still lie over P because PR_P lies over P. We have therefore reduced to the case when R is local with maximal ideal P. It now suffices to show that $PS \neq S$, since then any maximal ideal $\mathfrak{m} \subseteq S$ containing PS will be prime and contracts to an ideal containing P. Since P is maximal, this would imply that $\mathfrak{m} \cap R = P$.

It remains to show that $PS \neq S$. Consider the family of ideals

$$\Sigma = \left\{ I \subseteq R \,\middle|\, IS \neq S \right\}$$

partially ordered by inclusion. This set is nonempty since $(0) \in \Sigma$. The union of a chain in Σ is also in Σ for otherwise $1 \in S$ could be written as a sum of elements from finitely many members of that chain, and hence 1 would be contained in the largest member of that chain. By Zorn's Lemma 1.5.2, there is a maximal element $I \in \Sigma$. Now consider $IS \cap R = J$. Then, $I \subseteq J$, and since

$$JS \subseteq (IS \cap R)S \subseteq IS \neq S,$$

we see that $I = J$ by maximality. Thus, $R/I \to S/IS$ is injective and still integral, and R/I is still local. We may therefore replace $R \subseteq S$ by $R/I \subseteq S/IS$ to assume that Σ only contains (0), for if we show that $P(S/IS) \neq S/IS$, then we also have $PS \neq S$.

We now prove that $PS \neq S$ assuming that $\Sigma = \{(0)\}$. If $P = (0)$, we are done. By way of contradiction, we suppose that $P \neq (0)$. Choose $a \in P - \{0\}$. Since $\Sigma = \{(0)\}$, we know that $aS = S$. Thus, there exists $b \in S$ such that $ab = 1$. Since b is integral over R, there is an equation

$$b^n = r_{n-1}b^{n-1} + r_{n-2}b^{n-2} + \cdots + r_1 b + r_0.$$

Since $b = a^{n-1}$, we can multiply both sides by a^{n-1} to obtain

$$b = r_{n-1} + r_{n-2}a + \cdots + r_1 a^{n-2} + r_0 a^{n-1}$$

which shows that $a^{-1} = b \in R$. Thus, a has an inverse in R, contradicting the assumption that $a \in P$. □

4.4. Going up

We show the next Cohen–Seidenberg theorem.

[AK21, (14.3)(4)]
[Hoc17, p. 39]

THEOREM 4.4.1 (Going up). *Let $R \subseteq S$ be an integral extension of rings and consider a chain*

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

of prime ideals in R. Let Q_0 be a prime ideal of S lying over P_0. Then, there is a chain of prime ideals

$$Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_r$$

in S such that Q_t lies over P_t for every t.

The version of Going up in [CS46] is [CS46, Theorem 3].

Proof. We induce on r. The case $r = 0$ follows from lying over (Theorem 4.3.3(*ii*)). Now assume that the chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_{r-1}$ has been constructed. We can then consider the extension $R/P_{r-1} \subseteq S/Q_{r-1}$, which is integral as we saw in the proof of incomparability (Theorem 4.3.4(*ii*)). Since P_r/P_{r-1} is a prime ideal in R/P_{r-1}, there is a prime ideal lying over it (Theorem 4.3.3(*ii*)), which is of the form Q_r/Q_{r-1} for a prime ideal $Q_r \subset S$ by Proposition 1.3.12. Finally, Proposition 1.3.12 implies that this prime ideal Q_r lies over P_r as well. □

One important application of going up is that integral extensions preserve dimensions.

Corollary 4.4.2. *Let $R \subseteq S$ be an integral extension of rings. Then,* $\dim(R) = \dim(S)$. [AK21, (15.11)] [Hoc17, p. 40]

Proof. We first show $\geq$. Let $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_d$ be a chain of prime ideals in S. Then, each Q_t contracts to distinct primes P_t by incomparability (Theorem 4.3.4(*ii*)), and hence $\geq$ holds.

To show $\leq$, it suffices to note that for every chain of prime ideals in R, there is a chain of equal length in S by going up (Theorem 4.4.1). □

Remark 4.4.3. Corollary 4.4.2 implies that $\dim(k[t^2, t^3]) = 1$, which we were not able to show in Example 4.1.5.

One way to interpret the proof we just wrote down is in terms of height:

Definition 4.4.4. Let $P \subseteq R$ be a prime ideal in a ring R. The *height* $\mathrm{ht}(P)$ of P is the supremum of lengths r of strictly increasing chains

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

of prime ideals contained in P. Note that by Proposition 3.2.10, the height of P is the same as the Krull dimension of R_P.

We can now show:

Corollary 4.4.5. *Let $R \subseteq S$ be an integral extension of rings, and consider a prime ideal $Q \subseteq S$. Then,* $\mathrm{ht}(Q \cap R) \geq \mathrm{ht}(Q)$.

Proof. This is the same as the proof of $\geq$ in Corollary 4.4.2. □

We note that there exist examples where this inequality is strict.

Example 4.4.6. Consider the ring map [Hoc17, p. 47]

$$R = k[x] \subseteq \frac{k[x, y]}{(y - y^2, xy)} = S.$$

This is integral since S is generated by y over R, and y satisfies the monic equation $y^2 - y = 0$. It is also an extension since the ring map $S \to R$ sending $x \mapsto x$ and $y \mapsto 0$ is a retraction. Now consider

$$Q = (1 - y) \subseteq S.$$

This is a prime ideal in S since $S/Q \simeq k$. We claim that

$$\mathrm{ht}(Q) = 0 < 1 = \mathrm{ht}(Q \cap R).$$

We show the first equality, which says that Q is a minimal prime in S. Let $Q' \subseteq Q$ be a prime ideal. Then Q' is the image of a prime ideal $\tilde{Q}' \subseteq k[x,y]$ containing $y - y^2 = y(1-y)$. Such an ideal $\tilde{Q}'$ must contain y or $1-y$, but we see that $\tilde{Q}'$ cannot contain y (for otherwise Q would contain $y + (1-y) = 1$) and cannot contain $1-y$ (for otherwise $Q' = Q$).

For the second equality, we note that $Q \cap R$ contains x (since $x(1-y) = x - xy = x$), and hence $\operatorname{ht}(Q \cap R) \geq 1$. The height is equal to 1 since $\dim(R) = 1$.

We will start investigating later today under what assumptions height is preserved under integral maps.

4.5. Cardinality of fibers of module-finite maps

We have now seen how dimension changes under integral maps. We already saw how some of the most important examples of integral maps are normalizations. We will spend some time investigating how module-finite maps are reflected on spectra of rings.

EXAMPLE 4.5.1. Consider the ring $k[x,y]/(xy)$. This has an injection

$$R = \frac{k[x,y]}{(xy)} \hookrightarrow \frac{k[x,y]}{(xy,y)} \times \frac{k[x,y]}{(xy,x)} \simeq k[x] \times k[y] = S,$$

since $(x) \cap (y) = (0)$. The ring S is the integral closure of R in $k(x) \times k(y)$ since it is integral over R, and is integrally closed in $k(x) \times k(y)$ since any equation of integral dependence gives rise to two equations of integral dependence corresponding to each factor.

We investigate what prime ideals lie over the maximal ideal (x,y). We think it should be $(x) \times k[y]$ and $k[x] \times (y)$, which are maximal by Homework 0 (see also Proposition 1.7.1). But how do we rule out the existence of other prime ideals lying over (x,y)?

To investigate this sort of question in general, we introduce some terminology.

[Hoc17, pp. 40–41]

DEFINITION 4.5.2. Let $\varphi\colon R \to S$ be a ring map, and consider the associated map

$$g = \operatorname{Spec}(\varphi)\colon \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$$

on spectra. Borrowing terminology from topology, the *fiber* $g^{-1}(P)$ over a prime ideal $P \in \operatorname{Spec}(R)$ is the set of all prime ideals mapping to P under g. In other words, $g^{-1}(P)$ is the set of prime ideals in S lying over $P \in \operatorname{Spec}(R)$. This set of prime ideals is homeomorphic to the spectrum of

$$\frac{(R-P)^{-1}S}{P \cdot (R-P)^{-1}S} \simeq (R-P)^{-1}\frac{S}{PS}, \tag{4.5.3}$$

which is the same as localizing S/PS at the image of $R - P$ in S/PS. This ring is called the *fiber* of $R \to S$ over P, and is both an S-algebra and an R_P/PR_P-algebra. The primes in the fiber correspond to the primes of S that contain PS and are disjoint from $R - P$.

We will talk next time how to show (4.5.3) using the language of representable functors. For now, we note that the two sides in (4.5.3) satisfy the same universal properties.

Example 4.5.4. In the previous example, the fiber is

$$(R-(x,y))^{-1}\frac{k[x]\times k[y]}{((x,0),(0,y))}.$$

After some work, you can actually show that this isomorphic to $k[x]/(x)\times k[y]/(y)$.

Our goal, then, is to not have to do this work and still bound the number of prime ideals in a fiber.

We will also need the following. We recall that two ideals $I_1, I_2 \subseteq R$ are comaximal if $I_1 + I_2 = R$.

Theorem 4.5.5 (Chinese remainder theorem). *Let R be a ring, and consider pairwise comaximal ideals $I_1, I_2, \dots, I_n \subseteq R$ for $n \geq 2$ (i.e., for all $j \neq k$, we have $I_j + I_k = R$). Then, we have* [AK21, (1.13)] [Hoc17, p. 41]

$$J := I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n, \tag{4.5.6}$$

and the ideals $I_1 I_2, I_3, \dots, I_n$ are also pairwise comaximal. Moreover, the map

$$\frac{R}{J} \longrightarrow \frac{R}{I_1}\times\frac{R}{I_2}\times\cdots\times\frac{R}{I_n} \tag{4.5.7}$$

defined by $r + J \mapsto (r + I_1, r + I_2, \dots, r + I_n)$ is a ring isomorphism.

Proof. We proceed by induction. First consider the case when $n = 2$. The pairwise comaximality is vacuous, and hence it suffices to show (4.5.6) and that the map (4.5.7) is an isomorphism. The inclusion $I_1 \cdot I_2 \subseteq I_1 \cap I_2$ follows from definition of the product ideal. Conversely, if $j \in I_1 \cap I_2$, then writing $i_1 + i_2 = 1$ for $i_1 \in I_1$ and $i_2 \in I_2$, we have $j = j(i_1 + i_2) = ji_1 + ji_2 \in I_1 I_2$. This also shows the injectivity of (4.5.7), since the kernel is $I_1 \cdot I_2 = I_1 \cap I_2$. For surjectivity, if $(r_1 + I_1, r_2 + I_2)$ is in the codomain, then $r_1 i_2 + r_2 i_1$ maps to this element, where i_1, i_2 are as before, since

$$r_1 i_2 + r_2 i_1 \longmapsto (r_1 i_2 + I_1, r_2 i_1 + I_2) = (r_1 + I_1, r_2 + I_2)$$

since $r_1 i_1 \in I_1$ and $r_2 i_2 \in I_2$.

We now consider the inductive case. To show (4.5.6), it suffices to show that $I_1 I_2, I_3, \dots, I_n$ are pairwise comaximal by inductive hypothesis. It moreover suffices to show that $I_1 I_2$ is comaximal with I_j for each $j \geq 3$. Choose $i_1 \in I_1$ and $u \in I_j$ such that $i_1 + u = 1$, and choose $i_2 \in I_2$ and $v \in I_j$ such that $i_2 + v = 1$. Multiplying these two equations together, we have 9/13

$$\underbrace{i_1 i_2}_{\in I_1 I_2} + \underbrace{i_1 v + i_2 u + uv}_{\in I_j} = 1.$$

Now for (4.5.7), the inductive hypothesis and the $n = 2$ case imply

$$\frac{R}{J} = \frac{R}{(I_1 I_2) I_3 \cdots I_n} \xrightarrow{\sim} \frac{R}{I_1 I_2}\times\frac{R}{I_3}\times\cdots\times\frac{R}{I_n} \xrightarrow{\sim} \frac{R}{I_1}\times\frac{R}{I_2}\times\cdots\times\frac{R}{I_n}. \qquad \square$$

Example 4.5.8. The classical Chinese remainder theorem follows by considering $R = \mathbf{Z}$ and pairwise coprime integers $a_1, a_2, \dots, a_n$ which generate pairwise comaximal ideals $(a_1), (a_2), \dots, (a_n)$.

We can now answer the question we had about cardinality of fibers.

THEOREM 4.5.9. *Let R be a reduced k-algebra that is module-finite over a field k (and hence R is a finite-dimensional k-vector space). Then, R is a product of finite algebraic field extensions $L_1 \times L_2 \times \cdots \times L_n$ of K. The ring R has n maximal ideals, which are the kernels of the n projections $R \twoheadrightarrow L_i$ for $i \in \{1, 2, \ldots, n\}$, and the number of maximal ideals n is at most $\dim_k(R)$.* [Hoc17, p. 42]

Proof. Since $\dim(k) = 0$ and R is integral over k, we have $\dim(R) = 0$ by Corollary 4.4.2, and hence every prime ideal is maximal. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_h$ be any subset of maximal ideals of R. The Chinese Remainder Theorem 4.5.5 shows that

$$\frac{R}{\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_h} \simeq \frac{R}{\mathfrak{m}_1} \times \frac{R}{\mathfrak{m}_2} \times \cdots \times \frac{R}{\mathfrak{m}_h}.$$

Let $L_i = R/\mathfrak{m}_i$. Then, L_i is a field and is finite-dimensional as a k-vector space, and hence is a finite algebraic extension of k. As a k-vector space, $(R/\mathfrak{m}_1)\times(R/\mathfrak{m}_2)\times\cdots\times(R/\mathfrak{m}_h)$ is a direct sum over K of the fields L_i, which shows that h is at most the k-vector space dimension of $R/(\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_h)$, which is also at most the k-vector space dimension of R. Thus, the number of maximal ideals in R is bounded above by the k-vector space dimension of R. Now suppose that $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ are all the maximal ideals of R. Since R is reduced, the Scheinnullstellensatz (Theorem 1.5.7) implies that the intersection of the $\mathfrak{m}_i$ is zero. Thus, $R \simeq R/(0) \simeq R/\mathfrak{m}_1 \times R/\mathfrak{m}_2 \times \cdots \times R/\mathfrak{m}_n$. □

COROLLARY 4.5.10. *Let $R \to S$ be a module-finite ring map, where S is generated by n elements over R. Then, the number of prime ideals of S lying over a prime ideal $P \subseteq R$ is at most n.* [Hoc17, p. 42]

The following allows us to reduce to the local case:

LEMMA 4.5.11. *Let $R \to S$ be an integral (resp. module-finite) map. Then, the map $R_P/PR_P \to (R-P)^{-1}S/(P \cdot (R-P)^{-1}S)$ is integral (resp. module-finite).* [Hoc17, p. 41]

Proof. We already saw that integrality is preserved under localization in Lemma 4.3.6 and that it is preserved under quotienting by an ideal and its extension as in the proof of Incomparability (Theorem 4.3.4(*ii*)). The proof for module-finiteness is even simpler: if n elements generate S over R, then the same elements generate $(R-P)^{-1}S/(P \cdot (R-P)^{-1}S)$ over R_P/PR_P. □

Proof of Corollary 4.5.10. From Lemma 4.5.11 and the discussion about fibers above, we can replace $R \to S$ by $R_P/PR_P \to (R-P)^{-1}S/(P \cdot (R-P)^{-1}S)$. This does not increase the number n. Passing to $S/\sqrt{(0)}$ can only decrease its k-vector space dimension, while the number of prime ideals (which are all maximal) does not change. We can then apply Theorem 4.5.9. □

4.6. More on representable functors

One thing I want to revisit from before is why we have an isomorphism

$$\frac{(R-P)^{-1}S}{P \cdot (R-P)^{-1}S} \simeq (R-P)^{-1}\frac{S}{PS}$$

in the definition of the fiber ring. As I mentioned before, you can check they are isomorphic by checking they have the same universal property. Another way to see this is that they both represent the functor: They both represent the functor sending a ring T to the set of maps $\varphi\colon R \to T$ such that $\varphi(R-P)$ consists of units and $\varphi(P) = 0$.

The fact that objects representing the same functor are isomorphic is a consequence of the *Yoneda lemma*. A version of this lemma appears in [Yon54] but the current version was apparently first published in [Gro95] (which is a republication of a paper from 1960). The lemma is named after Nobuo Yoneda, who communicated the result to Mac Lane at a train station in 1954 [Kin98; Mac98].

LEMMA 4.6.1 (Yoneda [Yon54; Gro95, Proposition 1.1]). *Let $\mathcal{C}$ be a (locally small) category. Let $F\colon \mathcal{C}^{\mathrm{op}} \to \mathsf{Sets}$ be a functor. Then, for every object X of $\mathcal{C}$, there is a bijection* cf. [Hoc17, p. 40]

$$\begin{aligned} \left\{ \begin{matrix} \textit{natural transformations} \\ h_X \Rightarrow F \end{matrix} \right\} &\xrightarrow{\sim} F(X) \\ T &\longmapsto T_X(\mathrm{id}_X) \end{aligned} \tag{4.6.2}$$

that is natural in both X and F when both sides are considered as functors

$$\mathcal{C}^{\mathrm{op}} \times \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, \mathsf{Sets}) \longrightarrow \mathsf{Sets}.$$

Note that we defined all categories to be locally small (that is, to have Hom *sets*) in Definition 2.1.1.

Proof. Fix a morphism $f\colon Y \to X$ in $\mathcal{C}$. Then, we obtain a natural transformation

$$\begin{aligned} T^f &\colon h_X \Longrightarrow h_Y \\ (g\colon X \to Z) &\longmapsto (g \circ f\colon Y \to Z). \end{aligned}$$

Note that $h_X(X) \to h_Y(X)$ sends id_X to f.

We now consider the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(X,X) & \xrightarrow{T_X} & F(X) \\ {\scriptstyle T^f(X)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathrm{Hom}(Y,X) & \xrightarrow{T_Y} & F(Y) \end{array}$$

of sets, which exists by the naturality of T. Mapping id_X through each term in the commutative diagram, we have

$$\begin{array}{ccc} \mathrm{id}_X & \longmapsto & T_X(\mathrm{id}_X) \\ \downarrow & & \downarrow \\ f & \longmapsto & T_Y(f). \end{array}$$

We therefore see that the image of a natural transformation T in $F(X)$ is uniquely determined by the image $T_X(\mathrm{id}_X)$ of id_X since the naturality of T automatically determines how T transforms morphisms $f\colon Y \to X$. The fact that the image $T_X(\mathrm{id}_X)$ of id_X determines a natural transformation $T\colon h_X \Rightarrow F$ shows that (4.6.2) is surjective. The fact that the image $T_X(\mathrm{id}_X)$ of id_X *uniquely* determines a natural transformation $T\colon h_X \Rightarrow F$ shows that (4.6.2) is injective. □

As a consequence, we see the following:

COROLLARY 4.6.3. *Let $\mathcal{C}$ be a (locally small) category. Let X and Y be two objects in $\mathcal{C}$. If $h_X \cong h_Y$, then $X \cong Y$.* [Hoc17, p. 40]

Proof. The natural transformations $h_X \Rightarrow h_Y$ and $h_Y \Rightarrow h_X$ that compose to the identity in either order maps to two morphisms $Y \to X$ and $X \to Y$ that compose to the identity in either order by the Yoneda Lemma 4.6.1. □

4.7. Going down

We now return to the Cohen–Seidenberg theorems. We investigate when integral maps preserve height, as promised. This is the content of the following last Cohen–Seidenberg theorem:

[AK21, (14.9)] [Hoc17, p. 44]

THEOREM 4.7.1 (Going down). *Let R be a normal domain and let $R \subseteq S$ be an integral extension. Suppose that no nonzero element of R is a zerodivisor in S (i.e., that S is torsion-free as an R-module). Let*

$$P_r \supsetneq P_{r-1} \supsetneq \cdots \supsetneq P_0$$

be a chain of primes in R, and let Q_r be a prime ideal of S lying over P_r. Then, there is a chain of prime ideals

$$Q_r \supsetneq Q_{r-1} \supsetneq \cdots \supsetneq Q_0$$

in S such that Q_i lies over P_i for every i.

This result appeared as [CS46, Theorem 5] in Cohen and Seidenberg's paper. We note that the condition that S is torsion-free over R cannot be removed: the same example

$$R = k[x] \subseteq \frac{k[x,y]}{(y - y^2, xy)} = S.$$

from Example 4.4.6 does not satisfy going down.

We will need some preliminaries about polynomials.

[Hoc17, pp. 44–45]

PROPOSITION 4.7.2. *Let R be a ring, and consider the polynomial ring $R[x]$ in one variable over R.*

(*i*) *Let $f, g \in R[x]$ be nonzero polynomials of degree d and n and leading coefficients a and b. Then, if either a or b is not a zerodivisor in R, then the degree of fg is $d+n$ and its leading coefficient is ab. In particular, the conclusion holds if f or g is monic.*

(*ii*) *(Division algorithm) Let g be any polynomial, and let f be a monic polynomial in $R[x]$ of degree d. Then, one can write $g = qf + r$ where $q, r \in R[x]$ and either $r = 0$ or $\deg(r) < d$. This representation is unique.*

(*iii*) *Let $R \subseteq S$ be a ring extension and let $f, g \in R[x]$ as in (ii) with f monic. Then, g is a multiple of f in $R[x]$ if and only if it is a multiple of f in $S[x]$.*

Note that in (*i*), you can get products fg of smaller degree than expected, for example by considering $R = \mathbf{Z}/\langle 4 \rangle$ and the product $(\bar{2}x + 1)(\bar{2}x + 1) = 1$ in $R[x]$.

Proof. For (*i*), the product fg has at most one term of degree $d+n$, namely abx^{d+n}. This may or may not be zero, but definitely is not zero when either a or b is a nonzerodivisor.

For (*ii*), we perform long division in the usual way. More precisely, we proceed by induction on $n = \deg(g)$. If $g = 0$ or $\deg(g) < d$, then we set $q = 0$ and $r = g$. Otherwise, let ax^n be the leading term of g, where $a \in R - \{0\}$. Then

$g_1 = g - ax^{n-d}f$ has smaller degree than g, and so can be written in the form $q_1 f + r$ by inductive hypothesis. We then have

$$g = (ax^{n-d} + q_1)f + r$$

as required. For uniqueness, if $qf + r = q'f + r'$, then $(q - q')f = r - r'$ is zero or has degree smaller than that of f, which is impossible by (*i*) unless $q - q' = 0$, in which case $r - r' = 0$ as well.

Finally, for (*iii*), we can perform the division algorithm either in $R[x]$ or in $S[x]$. By uniqueness, the result is the same. If g is a multiple of f in $S[x]$, the remainder must be zero, and then the same holds in $R[x]$. □

The following result is why the "normal domain" assumption is necessary.

PROPOSITION 4.7.3. *Let R be a normal domain with fraction field K, and let S be a domain containing R. Suppose that $s \in S$ is integral over R. Let $f(x) \in K[x]$ be the minimal monic polynomial of s over K. Then, $f(x) \in R[x]$, and for any polynomial $g(x) \in R[x]$ such that $g(s) = 0$, we have $f(x) \mid g(x)$ in $R[x]$.* [Hoc17, p. 46]

Proof. Choose an algebraic closure $\mathrm{Frac}(S) \subseteq L$, in which case $K \subseteq L$ as well. The element s satisfies a monic polynomial $h(x)$ with coefficients in R. It follows that $f(x) \mid h(x)$ in $K[x]$, and hence every root of f in L is a root of $h(x)$. It follows that all roots of f are integral over R. The coefficients of f are elementary symmetric functions of the roots of f. Thus, the coefficients of f are elements of K that are integral over R. Since R is normal, they are in R.

Now suppose that $g(x) \in R[x]$ is a polynomial such that $g(s) = 0$. We know that $f(x) \mid g(x)$ in $K[x]$. The fact that $f(x) \mid g(x)$ in $R[x]$ then follows from Proposition 4.7.2(*iii*). □

Finally, we can show going down. 9/16

Proof of Going down (Theorem 4.7.1). Recall that we have an integral extension $R \subseteq S$ where R is a normal domain and where nonzero elements of R are not zerodivisors in S.

STEP 1. It suffices to consider the case when $r = 1$.

This is just by induction on the length of the chain, constructing one prime ideal at a time.

We can therefore change notation as follows: we are given a prime Q of S lying over P in R, and a prime $P_0 \subseteq P$ in R. We want to show that there is a prime $Q_0 \subseteq Q$ such that Q_0 lies over P_0.

STEP 2. Reduction to the case when S is also a domain.

We show that there is a prime ideal $\mathfrak{q} \subseteq S$ such that $\mathfrak{q} \subsetneq Q$ and $\mathfrak{q}$ lies over $(0) \subseteq R$. To do this, consider the multiplicative set

$$W = \big(R - \{0\}\big)(S - Q)$$

in S. Since the elements of $R - \{0\}$ are not zerodivisors in S and the elements of $S - Q$ are not zero, the multiplicative set W does not contain 0. This means there is a prime ideal $\mathfrak{q} \subseteq S$ disjoint from W by our application of Zorn's lemma (Proposition 1.5.5). In particular, since $R - \{0\} \subseteq W$, we see that $\mathfrak{q} \cap R = (0)$, and since $S - Q \subseteq W$, we must have $\mathfrak{q} \subseteq Q$. Since Q lies over P and $P_0 \subsetneq P$, we have that $P \neq (0)$, and hence $\mathfrak{q} \subsetneq Q$ by Incomparability (Theorem 4.3.4(*ii*)).

We now replace S by $S/\mathfrak{q}$. Since $\mathfrak{q} \cap R = \{0\}$, we still have an injection $R \hookrightarrow S/\mathfrak{q}$, and we may replace R by its image in $S/\mathfrak{q}$ to assume that $R \subseteq S/\mathfrak{q}$ is an integral extension of domains. If we find a prime of $S/\mathfrak{q}$ contained in $Q/\mathfrak{q}$ that lies over P_0, then it will have the form $Q_0/\mathfrak{q}$ for some prime of S with $Q_0 \subseteq Q$. Then, Q_0 will lie over P_0 in R and we will have $Q_0 \subseteq Q$. Since $P_0 \subsetneq P$, we actually have $Q_0 \subsetneq Q$.

Step 3. The special case when $R \subseteq S$ is an integral extension of domains, where R is normal.

Let $A = R - P_0$ and $B = S - Q$. To complete the proof, we will show that the multiplicative set AB does not meet the ideal P_0S. This implies that there is a prime ideal $Q_0 \subseteq S$ containing P_0S and disjoint from $AB \supseteq A \cup B$ again by Proposition 1.5.5, so that $P_0 \subseteq Q_0$ and Q_0 meets neither $R - P_0$ nor $S - Q$. But this means that Q_0 lies over P_0 and is contained in Q, as required.

We proceed by contradiction. Suppose that $a \in A$ and $b \in B$ are such that $ab \in P_0S$. By the application of the determinant trick we used to prove lying over (Lemma 4.3.1), we know that ab satisfies a monic polynomial equation $g_1(x) \in R[x]$ whose coefficients except the leading coefficient all lie in P_0. This means that b is a root of a polynomial $g(x) = g_1(ax)$ over $R[x]$, whose leading coefficient is a power of a.

We now think of $K = \mathrm{Frac}(R)$ as a subfield of $L = \mathrm{Frac}(S)$. Since b satisfies the algebraic equation $g(b) = 0$, it is algebraic over K, and has a monic minimal polynomial $f(x) \in K[x]$ that is irreducible in $K[x]$. By Proposition 4.7.3, this polynomial $f(x)$ has coefficients in R, since R is normal. It divides $g(x)$ in $K[x]$, since $g(x)$ has coefficients in $R \subseteq K$, and $f(x)$ is the *minimal* polynomial of b.

Now since $f(x)$ is monic, we can apply our version of the division algorithm (Proposition 4.7.2) to show that $f(x) \mid g(x)$ in $R[x]$ as well, in which case we have $g(x) = f(x)q(x)$ with $q(x) \in R[x]$. Considering the coefficients modulo P_0, since $a \in R - P$, its image $\bar{a} \in R/P$ is nonzero. Thus, modulo P_0, the polynomial $g(x)$ has the form $\bar{a}^d x^d$, since all lower coefficients are in P_0. This implies that the monic polynomial f must become x^k modulo P_0, where k is the degree of f. Thinking over R, this shows that $f(x)$ is monic of degree k with all lower coefficients in P_0:

$$f(x) = x^k + p_1 x^{k-1} + \cdots + p_k.$$

Finally, since b is a root of $f(x)$, we have

$$b^k = -p_1 b^{k-1} - \cdots - p_0 \in P_0 S \subseteq Q,$$

and hence $b \in Q$, a contradiction. This shows that AB does not meet P_0S. □

This shows the desired result about heights.

[Hoc17, p. 47] Corollary 4.7.4. *Let R be a normal domain, and let $R \subseteq S$ be an integral extension such that no nonzero element of R is a zerodivisor in S. Let $Q \subseteq S$ be a prime ideal. Then,* $\mathrm{ht}(Q \cap R) = \mathrm{ht}(Q)$.

Proof. We already saw that $\geq$ holds in Corollary 4.4.5 using Going up (Theorem 4.4.1). Conversely, given a chain of primes contained in $P = Q \cap R$ we can use Going down (Theorem 4.7.1) to show that the height of Q is at least as big as the height of P. □

We end with an example that shows that normality cannot be taken out of the assumptions in Going down (Theorem 4.7.1).

EXAMPLE 4.7.5. Let k be a field, and consider the ring extension [Hoc17, pp. 48–49]

$$R = k[x(1-x), x^2(1-x), y, xy] \subseteq k[x, y] = S.$$

The ring S is integral over R since it is generated over $k[y] \subseteq R$ by x, and x satisfies the monic polynomial $z^2 - z - x(1-x) = 0$, which has coefficients in R. The element $x \in R$ is in the fraction field of R, since

$$x = \frac{xy}{y} = \frac{x^2(1-x)}{x(1-x)} \in \mathrm{Frac}(R).$$

We now consider $Q = (1-x, y) \subseteq S$, which lies over

$$P = \big(x(1-x), x^2(1-x), y, xy\big) \subseteq R.$$

This ideal P is a maximal ideal in R. Now consider the contraction $P_0 = (x) \cap R$. We have that

$$P_0 = \big(x(1-x), xy\big) \subseteq R.$$

We claim that no prime Q_0 contained in Q lies over P_0. First, any prime of S contained in Q cannot contain x, since $x \notin Q$. But since Q_0 must contain both $x(1-x)$ and xy (since they are in P_0) and does not contain x, it must contain both $1-x$ and y. This forces Q_0 to equal Q, in which case it lies over P, not P_0.

CHAPTER 5

Noether's normalization theorem and Hilbert's Nullstellensatz

The next goal is to prove some very fundamental facts about rings finitely generated as algebras over fields. These are critical results in algebraic geometry. In commutative algebra, these sorts of results show why finitely generated algebras over fields are so well-behaved and nice to work with.

5.1. Algebraic sets

To motivate the two theorems we are proving next, we give some definitions from algebraic geometry.

DEFINITION 5.1.1. Let k be a field, and consider the n-fold product k^n of k. We say that a set $X \subseteq k^n$ is an *algebraic set* if there exists a set $\{f_i\}_{i \in I}$ of polynomials in $k[x_1, x_2, \ldots, x_n]$ such that [Rei95, (5.3)] [Hoc17, p. 4]

$$X = Z\big(\{f_i\}_{i \in I}\big) \coloneqq \big\{P = (a_1, a_2, \ldots, a_n) \in k^n \;\big|\; f_i(P) = 0 \text{ for all } i \in I\big\},$$

Here, we are thinking of $k[x_1, x_2, \ldots, x_n]$ as the ring of functions on k^n.

Closed algebraic sets are hard to draw over $\mathbf{C}$, and so we will usually draw them over $\mathbf{R}$ instead. See Figure 5.1 for some examples.

The two main theorems we will prove next have the following consequences:

(1) (Noether's normalization theorem, geometric version) Given an algebraic set $X \subseteq k^n$, there is a number $d \leq n$ and a change of coordinates on k^n such that the projection $k^n \to k^d$ induces a map $X \to k^d$ where the fiber over every point is nonempty and finite.

(2) (Hilbert's Nullstellensatz, geometric version) Suppose k is algebraically closed. Then, given an algebraic set $X = Z(I) \subseteq k^n$, the points

$$(a_1, a_2, \ldots, a_n) \in k^n$$

that lie in $Z(I)$ are in one-to-one correspondence with maximal ideals $(x_i - a_i)_{1 \leq i \leq n}$ that contain I.

We will prove more precise versions of these results.

5.2. Noether's normalization theorem

We start with Noether's normalization theorem. Our first goal is to show that after a change of variables, any nonzero polynomial in $R = k[x_1, x_2, \ldots, x_n]$ becomes a nonzero scalar times a polynomial that is monic in x_n with coefficients in $A = k[x_1, x_2, \ldots, x_{n-1}] \subseteq R$, where we think of R as $A[x_n]$. This will be key to our proofs of Noether's normalization theorem and Hilbert's Nullstellensatz.

We start by considering an example:

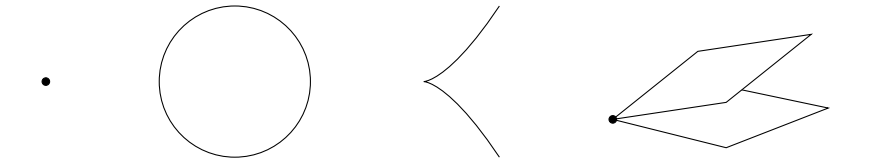


FIGURE 5.1. Some examples of algebraic sets in $\mathbf{R}^n$.

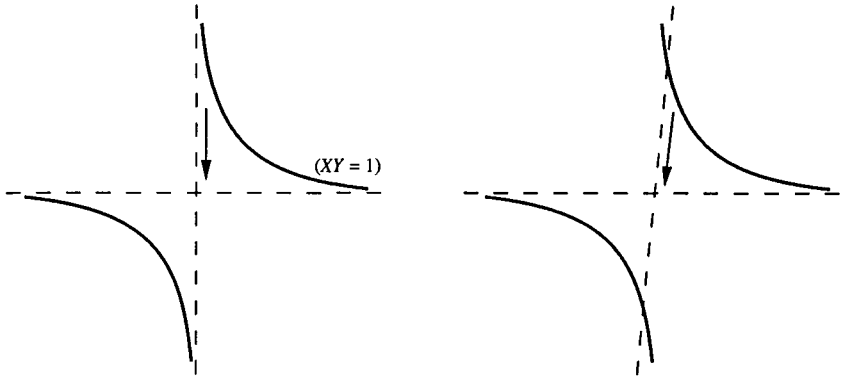


FIGURE 5.2. Projecting the hyperbola onto the x-axis has empty fibers, but has nonempty fibers after rotating the y-axis slightly. From [Rei95, Figure 4.8].

[Hoc17, p. 49]

EXAMPLE 5.2.1. Consider the polynomial $x_1x_2 \in k[x_1, x_2]$. There is then an automorphism of this polynomial ring such that $x_1 \mapsto x_1 + x_2$ and $x_2 \mapsto x_2$ (the inverse maps $x_1 \mapsto x_1 - x_2$ and $x_2 \mapsto x_2$). The image of x_1x_2 is $(x_1 + x_2)x_2 = x_2^2 + x_1x_2$, which is monic as a polynomial in x_2 over $k[x_1]$.

More generally, we note the following:

[Hoc17, p. 49]

REMARK 5.2.2. Let D be a ring, and let $R = D[x_1, x_2, \ldots, x_n]$ be the polynomial ring in n variables over D. Consider arbitrary elements

$$g_1(x_n), g_2(x_n), \ldots, g_{n-1}(x_n) \in D[x_n] \subseteq R.$$

Consider the assignment

$$x_i \longmapsto \begin{cases} x_i + g_i(x_n) & \text{if } i < n; \\ x_i & \text{if } i = n. \end{cases}$$

This defines an automorphism of R as a D-algebra with inverse

$$x_i \longmapsto \begin{cases} x_i - g_i(x_n) & \text{if } i < n; \\ x_i & \text{if } i = n. \end{cases}$$

[Rei95, (4.7)]
[Hoc17, p. 49]

LEMMA 5.2.3. *Let D be a domain and consider $f \in D[x_1, x_2, \ldots, x_n]$. Let $N \geq 1$ be an integer that is strictly larger than all of the exponents of the variables occurring*

in the terms of f. Let ϕ be the D-automorphism of $D[x_1, x_2, \ldots, x_n]$ defined by

$$x_i \longmapsto \begin{cases} x_i + x_n^{N^i} & \text{if } i < n; \\ x_i & \text{if } i = n. \end{cases}$$

Then, the image of f under ϕ is a polynomial whose sole highest degree term in x_n is a nonzero element $c \in D$ times a power of x_n. Thus, the image of f is a unit of D_c times a monic polynomial in x_n over $D_c[x_1, x_2, \ldots, x_{n-1}]$.

Proof. Consider any nonzero term of f of the form

$$c_\alpha x_1^{a_1} x_2^{a_2} \cdots x_{n-1}^{a_{n-1}} x_n^{a_n},$$

where $\alpha = (a_1, a_2, \ldots, a_n)$, and $c_\alpha \in D$ is nonzero. The image of this term under ϕ is

$$c_\alpha (x_1 + x_n^N)^{a_1} (x_2 + x_n^{N^2})^{a_2} \cdots (x_{n-1} + x_{n-1}^{N^{n-1}})^{a_{n-1}} x_n^{a_n}$$

and this contains a unique highest degree term in x_n, which is the product of the highest degree terms coming from all the factors, i.e.

$$c_\alpha (x_n^N)^{a_1} (x_n^{N^2})^{a_2} \cdots (x_{n-1}^{N^{n-1}})^{a_{n-1}} x_n^{a_n} = c_\alpha x_n^{a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1}}.$$

As α varies, the exponents that one gets on x_n in these largest degree terms coming from distinct terms of f are distinct because of the uniqueness of representations of integers in base N. Thus, no two exponents are the same, and no two of these terms can cancel, and the degree of the image of f is

$$m = \max_{\{\alpha | c_\alpha \neq 0\}} \left\{ a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1} \right\}.$$

Letting α_0 be the index that achieves this maximum m, we see that the term $c_{\alpha_0} x_n^m$ occurs in $\phi(f)$, and is the only term of degree m, and hence cannot be canceled. Thus, $c_{\alpha_0}^{-1} \phi(f)$ is monic of degree m in x_n when viewed as a polynomial in x_n over $D_c[x_1, x_2, \ldots, x_{n-1}]$, as required. □

Before we state Noether's normalization theorem, we state one definition.

Definition 5.2.4. Let R be an A-algebra and consider $z_1, z_2, \ldots, z_d \in R$. We say that the elements $z_1, z_2, \ldots, z_d$ are *algebraically independent* over A if the A-algebra map

$$\begin{aligned} A[x_1, x_2, \ldots, x_d] &\longrightarrow R \\ x_i &\longmapsto z_i \end{aligned}$$

is injective.

This is equivalent to the condition that the monomials $z_1^{a_1} z_2^{a_2} \cdots z_d^{a_d}$ as $\alpha = (a_1, a_2, \ldots, a_d) \in \mathbf{N}^d$ varies are all distinct and span a free A-submodule of R, which then would equal $A[z_1, z_2, \ldots, z_d]$. The failure of the z_j to be algebraically independent means that there is a nonzero polynomial $f(x_1, x_2, \ldots, x_d) \in A[x_1, x_2, \ldots, x_d]$ such that $f(z_1, z_2, \ldots, z_d) = 0$.

We now show the promised:

Theorem 5.2.5 (Noether's normalization theorem [Noe26]). *Let D be a domain and let R be a finitely generated D-algebra containing D. Then, there exists a nonzero element $c \in D$ and algebraically independent elements $z_1, z_2, \ldots, z_d$ in the D_c-algebra R_c such that R_c is module-finite over its subring $D_c[z_1, z_2, \ldots, z_d]$, which is isomorphic to a polynomial ring over D_c.* [AK21, (15.1)] [Rei95, (4.6)] [Hoc17, p. 50] [AM69, Exer. 5.20]

In particular, if D is a field k, then every finitely generated k-algebra is isomorphic to a module-finite extension of a polynomial ring over k.

9/18

Here, $d = 0$ is possible. The proof below is due to Nagata [Nag56, Chapter 1, §1].

Proof. Write

$$R = D[\theta_1, \theta_2, \dots, \theta_n].$$

We induce on the number n of generators of R over D. If $n = 0$, then $R = D$ and we can set $d = 0$.

Now suppose that $n \geq 1$ and that we know the result for algebras defined by at most $n-1$ elements. If the θ_i are algebraically independent over D then we are done: we can set $d = n$ and $z_i = \theta_i$ for every i. We may therefore assume that there exists a nonzero polynomial $f(x_1, x_2, \dots, x_n) \in D[x_1, x_2, \dots, x_n]$ such that $f(\theta_1, \theta_2, \dots, \theta_n) = 0$. Now instead of using the given generators for R as a D-algebra, we may use

$$\begin{aligned}
\theta_1' &= \theta_1 - \theta_n^N \\
\theta_2' &= \theta_2 - \theta_n^{N^2} \\
&\vdots \\
\theta_{n-1}' &= \theta_{n-1} - \theta_n^{N^{n-1}} \\
\theta_n' &= \theta_n
\end{aligned}$$

where N is chosen for f as in Lemma 5.2.3. With ϕ as in Lemma 5.2.3, these generators satisfy

$$g := \phi(f) = f\big(x_1 + x_n^N, x_2 + x_n^{N^2}, \dots, x_{n-1} + x_n^{N^{n-1}}, x_n\big).$$

Let $c \in D - \{0\}$ be the coefficient of the highest degree term of g in x_n. Then, over D_c, the polynomial $c^{-1}g$ is an equation of integral dependence for $\theta_n'/1$ over $S = D_c[\theta_1', \theta_2', \dots, \theta_{n-1}']$. This shows that R_c is module-finite over S by Lemma 4.2.3. Now by induction, there exists an element $c' \in D - \{0\}$ such that $S_{c'}$ is module-finite over $D_{c'}[z_1, z_2, \dots, z_d] \subseteq S_{c'}$. Noting that inverting c' and then c is the same as inverting cc', we have

$$D_{cc'} \subseteq D_{cc'}[z_1, z_2, \dots, z_d] \subseteq S_{cc'} \subseteq R_{cc'}$$

where the middle and right inclusions are module-finite by Lemma 4.5.11. □

This result has many corollaries!

[AK21, (15.4)]
[Hoc17, p. 51]
[AM69, Exer. 5.18]

Corollary 5.2.6 (Zariski's Nullstellensatz [Zar47, p. 363]). *Let R be a finitely generated algebra over a field k, and suppose that R is a field. Then, R is a finite algebraic extension of k, and in particular, R is module-finite over k.*

Proof. By Noether's Normalization Theorem 5.2.5, we know that R is module-finite over some polynomial subring $k[z_1, z_2, \dots, z_d] \subseteq R$. If $d \geq 1$, this polynomial ring has dimension at least one, in which case $\dim(R) \geq 1$ by Corollary 4.4.2, which would contradict the assumption that R is a field. Thus, we have $d = 0$, and R is module-finite over k itself. Since R is a field, this is the same as saying that R is a finite algebraic extension of k. □

[Hoc17, p. 54]

Corollary 5.2.7. *Let $R \to S$ be a homomorphism of finitely generated k-algebras. Then, every maximal ideal of S contracts to a maximal ideal of R. Thus, the maximal spectrum* MaxSpec *defines a functor*

$$\mathrm{MaxSpec}\colon \left(\mathsf{Alg}_k^{\mathrm{fg}}\right)^{\mathrm{op}} \longrightarrow \mathsf{Sets}.$$

Proof. Let $\mathfrak{n} \subseteq S$ be a maximal ideal with contraction $P \subseteq R$. We then obtain a composition

$$k \subseteq R/P \subseteq S/\mathfrak{n}.$$

By Corollary 5.2.6, $S/\mathfrak{n}$ is a finite algebraic extension of k. In particular, $S/\mathfrak{n}$ is a finite-dimensional k-vector space. Since R/P is a sub-k-vector space of $S/\mathfrak{n}$, it is also finite-dimensional as a k-vector space, and is module-finite over k. This means that $\dim(R/P) = 0$ by Corollary 4.4.2. Since R/P is a domain, it therefore must be a field. □

Corollary 5.2.8. *Let k be an algebraically closed field, let R be a finitely generated k-algebra, and let $\mathfrak{m} \subseteq R$ be a maximal ideal. Then, the composition* [Hoc17, p. 51]

$$k \longrightarrow R \twoheadrightarrow R/\mathfrak{m}$$

is an isomorphism.

Proof. The codomain $R/\mathfrak{m}$ is a finitely generated k-algebra, since R is, and it is a field. Corollary 5.2.6 then shows that $k \to R/\mathfrak{m}$ is a finite algebraic extension. Since k is algebraically closed, it has no proper algebraic extensions, and hence $k \to R/\mathfrak{m}$ must be an isomorphism. □

5.3. Hilbert's Nullstellensatz

We can now show a weak form of Hilbert's Nullstellensatz as a corollary to Noether normalization. We will focus on the case when k is algebraically closed field, although there are versions of some of these results without this assumption.

Corollary 5.3.1 (Hilbert's Nullstellensatz, weak form). *Let $R = k[x_1, x_2, \ldots, x_n]$ be a polynomial ring over an algebraically closed field k. Then, every maximal ideal $\mathfrak{m} \subseteq R$ is the kernel of a k-algebra map* [Hoc17, p. 51]

$$\begin{aligned} \varphi\colon k[x_1, x_2, \ldots, x_n] &\longrightarrow k \\ x_i &\longmapsto \lambda_i \end{aligned}$$

defined by evaluating a polynomial $f(x_1, x_2, \ldots, x_n)$ at the point $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in k^n$. This kernel is the same as the ideal

$$(x_1 - \lambda_1, x_2 - \lambda_2, \ldots, x_n - \lambda_n) \subseteq R.$$

Proof. Let $\mathfrak{m} \subseteq R$ be a maximal ideal. The composition of k-algebra maps

$$\gamma\colon k \longrightarrow R \twoheadrightarrow R/\mathfrak{m}$$

is an isomorphism by Corollary 5.2.8. The composition

$$R \longrightarrow R/\mathfrak{m} \xrightarrow[\sim]{\gamma^{-1}} k$$

then gives a map $\varphi\colon R \to k$ whose kernel is $\mathfrak{m}$. Such a map is determined by where the x_i map to, and setting $\varphi(x_i) = \lambda_i$ as in the statement of the corollary, we see that

$$(x_1 - \lambda_1, x_2 - \lambda_2, \ldots, x_n - \lambda_n) \subseteq \mathfrak{m}.$$

But the ideal on the left-hand side is maximal since the quotient of R by this ideal is k. □

[Hoc17, p. 52] This shows that there is a bijection

$$k^n \longleftrightarrow \operatorname{MaxSpec}\big(k[x_1, x_2, \dots, x_n]\big).$$

The Zariski topology determined by saying $Z(I) \subseteq k^n$ are closed for ideals $I \subseteq k[x_1, x_2, \dots, x_n]$ is the same as the subspace topology when thinking of MaxSpec as a subset of Spec.

The following result says that algebraic sets $Z(I)$ can detect whether $1 \in I$.

[Hoc17, p. 51] Corollary 5.3.2 (Hilbert's Nullstellensatz, alternative weak form). *Let k be an algebraically closed field, and consider polynomials*

$$f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n] = R.$$

Then, the f_i generate the unit ideal (i.e., there exist polynomials g_t for which $1 = \sum_t g_t f_t$) if and only if the polynomials do not vanish simultanenously, i.e., if and only if

$$Z(f_1, f_2, \dots, f_m) = \emptyset.$$

Proof. We prove $\Leftarrow$ by contrapositive. If the f_i do not generate the unit ideal, then the ideal they generate is contained in a maximal ideal $\mathfrak{m} \subseteq R$. But Corollary 5.3.1 shows that there exists a point $(\lambda_1, \lambda_2, \dots, \lambda_n) \in k^n$ for which all the f_i vanish.

We now show $\Rightarrow$. If the f_i all vanish at a point of $(\lambda_1, \lambda_2, \dots, \lambda_n) \in k^n$, then they are contained in the maximal ideal determined by that point as in Corollary 5.3.1. This direction does not need the assumption that k is algebraically closed. □

We can now show the strong form of Hilbert's Nullstellensatz.

[AK21, (15.7)] [Hoc17, p. 52] Theorem 5.3.3 (Hilbert's Nullstellensatz [Hil1893, pp. 320–321]). *Let k be an algebraically closed field, and consider the polynomial ring $R = k[x_1, x_2, \dots, x_n]$ in n variables over k. Suppose $g, f_1, f_2, \dots, f_s \in R$. Then, $g \in \sqrt{(f_1, f_2, \dots, f_s)}$ if and only if $Z(g) \supseteq Z(f_1, f_2, \dots, f_s)$, i.e., if and only if g vanishes at every point where the f_i vanish simultaneously.*

Proof. For $\Rightarrow$, it suffices to note that we can write

$$g^N = \sum_{i=1}^{s} g_i f_i$$

for some N and for some $g_i \in R$, and hence g vanishes at every point where the f_i vanish: we have $g(y)^N = 0$ at such a point, and hence $g(y) = 0$ since k is a field.

We now show $\Leftarrow$, using what is known as Rabinowitsch's trick [Rab30].[1] Suppose that g vanishes at every point where the f_i vanish. If $g = 0$, then there is nothing to show, and hence we will assume that $g \neq 0$. We introduce another variable z and consider the polynomials

$$f_1, f_2, \dots, f_s, 1 - gz \in k[x_1, x_2, \dots, x_n, z] = R[z].$$

Then, there is no point of k^{n+1} where these polynomials all vanish: at any point where the f_i vanish, we have that g vanishes as well, and therefore $1 - gz$ evaluates to

[1] See [Pal04] for some historical background.

$1 - 0 = 1$. By Corollary 5.3.2, this means that the polynomials $f_1, f_2, \ldots, f_s, 1 - gz$ generate the unit ideal in $k[x_1, x_2, \ldots, x_n, z]$. There is therefore an equation

$$1 = H_1(z)\, f_1 + \cdots + H_s(z)\, f_s + H(z)\,(1 - gz) \tag{5.3.4}$$

where we think of $H_i(z) \in R[z]$ as polynomials in z with coefficients in R for all i. We now define an R-algebra map

$$\begin{aligned} \varphi\colon R[z] &\longrightarrow R[1/g] = R_g \\ z &\longmapsto 1/g \end{aligned}$$

Applying φ to (5.3.4), we obtain

$$1 = H_1(1/g)\, f_1 + \cdots + H_s\,(1/g) f_s + H(1/g)\,(1 - 1).$$

The last term vanishes, yielding

$$1 = H_1(1/g)\, f_1 + \cdots + H_s\,(1/g) f_s.$$

Since $H_i(1/g) \in R_g$ for every i, there exists a power g^N of g such that $g_i = g^N H_i(1/g) \in R$ by clearing all of their denominators. Multiplying by g^N gives

$$g^N = g_1 f_1 + \cdots + g_s f_s. \qquad \square$$

THEOREM 5.3.5. *Let k be a field, and consider a finite type k-algebra R. For every proper finitely generated ideal $I \subsetneq R$, we have* [AK21, (15.6)] [Hoc17, p. 60]

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{m}} \mathfrak{m}.$$

Proof. The inclusion "$\subseteq$" holds since $I \subseteq \mathfrak{m}$ for every $\mathfrak{m}$. It therefore suffices to show "$\supseteq$". By the Scheinnullstellensatz (Theorem 1.5.7), it suffices to prove the statement when I is a prime ideal $P \subseteq R$.

STEP 1. Reduction to the case when R is a domain and $P = (0)$.

Suppose we have an element $u \in \bigcap_{P \subseteq \mathfrak{m}} \mathfrak{m}$. The special case when R is a domain and $P = (0)$ implies that the image $\bar{u} \in R/P$ of u lies in the intersection of every maximal ideal in R/P, and hence $\bar{u} = 0$. This shows that $u \in P$.

STEP 2. Reduction to the case when $R = k[x_1, x_2, \ldots, x_d]$ and $P = (0)$.

By way of contradiction, suppose that $u \in \bigcap_{\mathfrak{m}} \mathfrak{m}$ is nonzero. By the Noether normalization Theorem 5.2.5, the ring R is module-finite over a polynomial ring $A = k[x_1, x_2, \ldots, x_d]$ and a nonzero multiple of u lies in A by Theorem 4.3.4(i). We may therefore assume that $u \in A - \{0\}$. Since every maximal ideal of R lies over a maximal ideal of A by Going Up (Theorem 4.4.1), we obtain a counterexample in A.

STEP 3. The case when $R = k[x_1, x_2, \ldots, x_d]$ and $P = (0)$.

Let $\bar{k}$ be an algebraic closure of k. Since $u \neq 0$, there exists a maximal ideal $\mathfrak{m} \subseteq \bar{k}[x_1, x_2, \ldots, x_d]$ corresponding to a point $(\lambda_1, \lambda_2, \ldots, \lambda_d) \in \bar{k}^d$ such that $u(\lambda_1, \lambda_2, \ldots, \lambda_d) \neq 0$. The λ_i live in a finite algebraic extension k' of k, and evaluation at $(\lambda_1, \lambda_2, \ldots, \lambda_d)$ gives a surjection

$$k[x_1, x_2, \ldots, x_d] \twoheadrightarrow k[\lambda_1, \lambda_2, \ldots, \lambda_d]$$

that does not kill u. The kernel of this map is a maximal ideal not containing u. $\square$

We also write down a slightly different proof, which uses similar ideas but reduces to the case when k is algebraically closed in a different way.

Alternative Proof of Theorem 5.3.5. We first note that it suffices to consider the case when R is a polynomial ring by taking a surjection $k[x_1, x_2, \ldots, x_n] \twoheadrightarrow R$, proving the result for the contraction of I, and then taking images.

We now reduce to the case where k is algebraically closed. The map

$$R = k[x_1, x_2, \ldots, x_n] \subseteq \overline{k}[x_1, x_2, \ldots, x_n] = S$$

is an integral extension, since if $a_\lambda \in \overline{k}$ generate $\overline{k}$ over k, then $a_\lambda x_i$ generate S over R. If we can write

$$\sqrt{\sqrt{I}S} = \sqrt{IS} = \bigcap_{IS \subseteq \mathfrak{m} \subseteq S} \mathfrak{m}$$

in S, then we can write

$$\sqrt{\sqrt{I}S} \cap R = \bigcap_{IS \subseteq \mathfrak{m} \subseteq S} (\mathfrak{m} \cap R).$$

We can write the left-hand side as

$$\sqrt{\sqrt{I}S} \cap R = \sqrt{\sqrt{I}S \cap R} = \sqrt{\sqrt{I}},$$

where the first equality is [AK21, (3.22)] (cf. Corollary 1.4.7), and the second equality is the preliminary result we proved in Lying over (Theorem 4.3.3(i)). We therefore have

$$\sqrt{I} = \bigcap_{IS \subseteq \mathfrak{m} \subseteq S} (\mathfrak{m} \cap R).$$

It remains to show the right-hand side contracts to the correct thing in R. But this follows since all maximal ideals in R containing I have a maximal ideal lying over them by Lying over (Theorem 4.3.3(ii)), which contain IS by definition, and the contractions of such ideals are maximal by Going up (Theorem 4.4.1).

Finally, we prove the corollary when $R = k[x_1, x_2, \ldots, x_n]$ for an algebraically clsoed field k. The Scheinnullstellensatz (Theorem 1.5.7) implies

$$\sqrt{I} = \bigcap_{I \subseteq P} P \subseteq \bigcap_{I \subseteq \mathfrak{m}} \mathfrak{m}.$$

The inclusion is in fact an equality by Hilbert's Nullstellensatz (Theorem 5.3.3), which we can see as follows:

$$\begin{aligned} g \in \sqrt{I} &\iff Z(g) \supseteq Z(I) \\ &\iff \text{for every } \mathfrak{m} \supseteq I, \text{ we have } g \in \mathfrak{m} \\ &\iff \text{for every } \mathfrak{m} \supseteq I, \text{ we have } Z(g) \supseteq Z(\mathfrak{m}) \\ &\iff g \in \bigcap_{I \subseteq \mathfrak{m}} \mathfrak{m}. \end{aligned}$$

□

5.4. Effective Nullstellensatz (not covered in class)

I want to mention an additional aspect of Hilbert's Nullstellensatz. You can ask whether given the degrees of the f_i, one can bound the degrees of the g_i. This was first considered by Hermann [Her26], with later contributions of Masser and Wüstholz [MW83], by Thompson [Tho86, Theorems 2.1 and 2.1′], and by Shiffman [Shi89]. These bounds were doubly exponential.

In 1987, Brownawell [Bro87] found exponential bounds in characteristic zero. In 1988, Kollár [Kol88] proved the following effective version of the weak Nullstellensatz:[2]

THEOREM 5.4.1 (Effective Nullstellensatz; see [Kol88, Theorem 1.5]). *Let k be a field, and consider polynomials*

$$f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$$

in $n \geq 2$ variables of degrees $d_s \geq d_{s-1} \geq \cdots \geq d_1$. If the f_i generate the unit ideal, we can write

$$1 = g_1 f_1 + g_2 f_2 + \cdots + g_s f_s$$

where

$$\deg(g_i f_i) \leq \max\{d_s, 3\} \prod_{j=1}^{\min\{n,s\}-1} \max\{d_j, 3\}.$$

There is a version of Kollár's bound for the full Nullstellensatz as well.

There have been other bounds proved since then. For example, there are also bounds due to Sombra [Som99] of the form

$$\deg(g_i f_i) \leq 2 d_s \prod_{j=1}^{\min\{n,s\}-1} d_j,$$

which are an improvement if at least two of the d_j are less than 3.

5.5. Dimension theory for k-algebras

Now that we have Noether's Normalization Theorem 5.2.5, we can compute the dimension of polynomial rings over fields. We start with a definition: 9/20

DEFINITION 5.5.1. Let R be a ring. A chain of prime ideals [Hoc17, p. 54]

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

in R is *saturated* if for all $i \in \{0, 1, \dots, r-1\}$, there is no prime ideal strictly between P_i and P_{i+1}.

We can now state:

THEOREM 5.5.2. *Let k be a field and let R be a domain that is finitely generated as a k-algebra. Choose $z_1, z_2, \dots, z_d \in R$ such that R is module-finite over the polynomial ring $A = k[z_1, z_2, \dots, z_d]$. We have the following:* [AK21, (15.8), (15.13)] [Hoc17, p. 54]

(*i*) $\dim(R) = d$.
(*ii*) *For every maximal ideal $\mathfrak{m} \subseteq R$, we have* $\operatorname{ht}(\mathfrak{m}) = d$.
(*iii*) *Every saturated chain of prime ideals from* (0) *to a maximal ideal $\mathfrak{m}$ has length d.*

The conditions in (*ii*) and (*iii*) are called *equicodimensional* and *biequidimensional*, respectively. While these definitions are originally from [EGAIV$_1$, Chapitre 0, Définition 14.2.1] and [EGAIV$_1$, Chapitre 0, Proposition 14.3.3], respectively, the latter proposition is incorrect. This was noticed only recently by Gabber and Chen (independently; see [ILO14, Exposé XIV, §2.4]), and by Heinrich (also independently) in [Hei17].

[2] This exact statement is taken from Wikipedia.

To prove Theorem 5.5.2, we need the following:

[AK21, (21.14)]
[Hoc17, p. 54]

LEMMA 5.5.3. *Let R be a UFD. Then, every nonzero prime ideal of R contains a prime ideal generated by an irreducible element, and a prime ideal has height one if and only if it is generated by an irreducible element.*

Proof. Let Q be a nonzero prime ideal, and let $f \in Q - \{0\}$. Then, f can be written as a product of irreducible factors

$$f = f_1 f_2 \cdots f_n.$$

Since Q is prime, at least one of the f_i lies in Q. Then, f_i generates a prime ideal contained in Q. This also shows that if a prime ideal has height one, then it must be generated by an irreducible element.

Conversely, suppose $P = (f)$ for an irreducible element $f \in R$. We want to show that every nonzero prime ideal $Q \subseteq P$ is in fact equal to P. By the first part of this lemma, there exists a nonzero irreducible element g such that

$$(g) \subseteq Q \subseteq P = (f).$$

But this implies that $f \mid g$. Since both f and g are irreducible, they must differ by a unit factor, and hence $(g) = (f)$, which implies $Q = P$. □

We can now prove Theorem 5.5.2.

Proof of Theorem 5.5.2. We first show (*i*). Since $\dim(R) = \dim(A)$ by Corollary 4.4.2, it suffices to replace R by A to reduce to the case of a polynomial ring. We have already seen that $\dim(A) \geq d$. For the opposite inequality, we proceed by induction. We already know that $\dim(k) = 0$. If $d \geq 1$, consider a chain of prime ideals in A. After possibly making it longer, we can assume that it starts with

$$(0) \subsetneq P,$$

where P is a height one prime generated by an irreducible element f using Lemma 5.5.3. The image of this chain in A/P will have length one less in A/P, and hence it suffices to show that $\dim(A/P) \leq d-1$. After a change of coordinates (use Lemma 5.2.3), we may assume that f is monic in z_d over $k[z_1, z_2, \ldots, z_{d-1}]$, and hence A/P is integral over $k[z_1, z_2, \ldots, z_{d-1}]$. By inductive hypothesis and by using Corollary 4.4.2 again, we see that $\dim(A/P) \leq d-1$, and hence $\dim(A) \leq d$.

Since (*ii*) follows from (*iii*), it suffices to show the latter. We can proceed as in the proof of (*i*), but we will need to use Going Down (Theorem 4.7.1). We again proceed by induction on d. When $d = 0$, the ring R is a finite field extension of k by Zariski's Nullstellensatz (Corollary 5.2.6), and hence it suffices to consider the case when $d \geq 1$. Fix a maximal ideal $\mathfrak{m} \subseteq R$ and consider a saturated chain

$$(0) \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_r = \mathfrak{m}.$$

We want to show that $r = d$. Since the chain is saturated, we know that $\mathrm{ht}(Q_1) = 1$. By the corollary to Going Down (Corollary 4.7.4), we know that $\mathrm{ht}(Q_1 \cap A) = 1$, and hence must be generated by an irreducible element $f \in A$ by Lemma 5.5.3. As before, after a change of coordinates (use Lemma 5.2.3), we may assume that f is monic in z_d over $k[z_1, z_2, \ldots, z_{d-1}]$. Now

$$(0) = Q_1/Q_1 \subsetneq Q_2/Q_1 \subsetneq \cdots \subsetneq Q_r/Q_1 = \mathfrak{m}/Q_1$$

is a saturated chain of prime ideals of length $r-1$ in R/Q_1 from (0) to $\mathfrak{m}/Q_1$. Since R/Q_1 is module-finite over $A/(f)$, which is module-finite over $k[z_1, z_2, \ldots, z_{d-1}]$, we know that

$$\dim(R/Q_1) = \dim\big(A/(f)\big) = \dim\big(k[z_1, z_2, \ldots, z_{d-1}]\big) = d-1.$$

By inductive hypothesis, we therefore have $r-1 = d-1$, and hence $r = d$. □

As a consequence, we can compute dimensions of finitely generated algebras over fields using field theory. Before we state this result, we review the notion of transcendence degree from field theory.

Definition 5.5.4. Let $K \subseteq L$ be a field extension. By Zorn's Lemma 1.5.2, any set of elements in L algebraically independent over K can be enlarged to a maximal such set. Such a set is called a *transcendence basis* for L over K. [Hoc17, p. 55]

If $\{x_\lambda\}_{\lambda\in\Lambda}$ is a transcendence basis for L over K, then we have inclusions

$$K \subseteq K[x_\lambda]_{\lambda\in\Lambda} \subseteq K(x_\lambda)_{\lambda\in\Lambda} \subseteq L.$$

The field extension $K \subseteq K(x_\lambda)_{\lambda\in\Lambda}$ is a *pure transcendental extension* of K. The extension $K(x_\lambda)_{\lambda\in\Lambda} \subseteq L$ is algebraic, for otherwise we could enlarge the transcendence basis $\{x_\lambda\}_{\lambda\in\Lambda}$ further.

Theorem 5.5.5. *Let $K \subseteq L$ be a field extension. Then, any two transcendence bases for L over K have the same cardinality.* [Hoc17, p. 56] [Lan02, Thm. VIII.1.1] [DF04, p. 645]

Proof. We will show that if X is a set of algebraically independent elements of L and Y is a transcendence basis, then there exists an injection $f\colon X \hookrightarrow Y$ such that

$$X \cup \big(Y - f(X)\big)$$

is a transcendence basis for L over K. By symmetry, this will show that any two transcendence bases have the same cardinality.

Consider all injections $g\colon X_0 \hookrightarrow Y$, where X_0 is a (possibly empty) subset of X such that

$$X_0 \cup \big(Y - g(X_0)\big)$$

is a transcendence basis for L over K. These injections are partially ordered by $(X_0, g_0) \preceq (X_1, g_1)$ if $X_0 \subseteq X_1$ and $g_1|_{X_0} = g_0$. Every chain $(X_i, g_i)_{i\in I}$ has an upper bound in this partially ordered set: there is a unique function g on $X = \bigcup_i X_i$ extending all the given functions, and

$$X \cup \big(Y - g(X)\big)$$

is a transcendence basis for L over K (because any element of L is algebraic over a field generated by finitely many $y_j \in Y$, and these y_j will be replaced by x_k for sufficiently large X_i). By Zorn's Lemma 1.5.2 again, there is a maximal pair (X_0, g) in this partially ordered set.

We claim that $X_0 = X$. If not, choose $x \in X - X_0$. Then, x is algebraic over

$$K\big(X_0 \cup \big(Y - g(X_0)\big)\big),$$

and hence satisfies a polynomial equation over this field. Clearing denominators, we obtain a polynomial F over K in x and finitely many of the variables in $X_0 \cup (Y - g(X_0))$ such that x occurs in F. The polynomial F involves at least one element of $Y - g(X_0)$, for otherwise X would not be algebraically independent. We

can therefore choose $y \in Y - g(X_0)$ that occurs in F. But then, y is algebraic over the field generated over K by

$$X_0 \cup \{x\} \cup \big(Y - g(X_0) - \{y\}\big),$$

and we can extend g to g' on $X_1 = X \cup \{x\}$ by letting $g'(x) = y$. We still have algebraic independence since x is the only element that has been changed, and if an algebraic relation involves x, then x is algebraic over the field generated by the other elements, which implies that y is also algebraic over the field generated by the other elements, a contradiction. Finally, L is algebraic over the field generated by these elements because y is algebraic over this field. □

We can therefore make the following:

[Hoc17, p. 55] Definition 5.5.6. Let $K \subseteq L$ be a field extension. The *transcendence degree* of L over K is the maximum cardinality of a set of algebraically independent elements in L over K.

[AK21, (15.12)] [Hoc17, p. 56] Corollary 5.5.7. *Let k be a field and let R be domain that is finitely generated as a k-algebra. Then,* $\dim(R) = \operatorname{trdeg}_k(\operatorname{Frac}(R))$.

Proof. By Noether's Normalization Theorem 5.2.5, we have a factorization

$$k \subseteq k[z_1, z_2, \ldots, z_d] \subseteq R,$$

where the latter extension is module-finite, and where $d = \dim(R)$ by Theorem 5.5.2(i). Now taking fraction fields, we obtain a sequence

$$k \subseteq k(z_1, z_2, \ldots, z_d) \subseteq \operatorname{Frac}(R),$$

where the first extension is purely transcendental, and the second extension is algebraic. □

5.6. Valuation rings

9/23

We mentioned above that finitely generated domains over fields have nicely behaved spectra. We want to give an example of a ring where heights of maximal ideals can differ. To do so, we introduce an important class of rings that we will see again later.

[Hoc17, p. 57] [AK21, (23.1), (23.6)] Definition 5.6.1. A *discrete rank one valuation domain* or *DVR* is a principal ideal domain (PID) that is local.

Example 5.6.2.

(1) Any localization of a PID at a prime ideal is a DVR. In particular, $\mathbf{Z}_{(p)}$ is a DVR.
(2) The formal power series ring $k[\![t]\!]$ is a DVR.

Now let V be a DVR with maximal ideal (t). Then, since t is the only prime element up to multiplication by units, every nonzero element $f \in V$ can be written as αt^n where α is a unit in V. The non-negative integer n is called the *order* of f, written $\operatorname{ord}(f)$, and the function $\operatorname{ord}\colon \operatorname{Frac}(V) - \{0\} \to \mathbf{Z}$ is called the *valuation* associated to V. For nonzero $f, g \in V$, the order satisfies

$$\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g),$$

and if $f+g \neq 0$ as well, we have

$$\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}$$

with equality if $\operatorname{ord}(f) \neq \operatorname{ord}(g)$. Conversely, given a field F and a surjective function $\operatorname{ord}\colon F - \{0\} \to \mathbf{Z}$ such that these two properties hold, then

$$V \coloneqq \{f \in F \mid \operatorname{ord}(f) \geq 0\} \cup \{0\}$$

is a subring of F. It is a DVR with maximal ideal

$$\mathfrak{m} \coloneqq \{f \in F \mid \operatorname{ord}(f) > 0\} \cup \{0\}$$

which is generated by any element $t \in \mathfrak{m}$ of order 1. Every element in $\mathfrak{m}$ is of the form αt^n. Thus, every order function on a field F determines a unique DVR for which it is the associated valuation.

We now give an example:

Example 5.6.3. Let V be a DVR with maximal ideal (t). In the ring $V[x]$, which is a UFD, the element $tx-1$ generates a maximal ideal since $V[x]/(tx-1) \simeq V[1/t] = \operatorname{Frac}(V)$. On the other hand, the chain [Hoc17, p. 59]

$$(0) \subsetneq (x) \subsetneq (x,t)$$

shows that $\operatorname{ht}((x,t)) \geq 2$.

5.7. Back to dimension theory

If you are not a domain, you can also construct examples over fields:

Example 5.7.1. Let k be a field, and consider the ring [Hoc17, p. 59]

$$R = \frac{k[x,y,z]}{(xy,xz)}.$$

In this ring, every prime ideal contains either $\bar{x}$ or both $\bar{y}$ and $\bar{z}$. Thus, $P = (\bar{x})$ is a minimal prime with $R/P \simeq k[y,z]$, and $P' = (\bar{y},\bar{z})$ is a minimal prime with $R/P' \simeq k[x]$. Saturated chains from P to a maximal ideal correspond to a saturated chain in $k[y,z]$ and hence have length two. Saturated chains from P' to a maximal ideal correspond to a saturated chain in $k[x]$ and hence have length one.

Geometrically, since $(xy,xz) = (x) \cap (y,z)$, we can think of $\operatorname{MaxSpec}(R)$ as the union of the yz-plane and the x-axis in k^3.

On the other hand, we do have the following:

Theorem 5.7.2. *Let R be a finitely generated algebra over a field k. We then have the following:* [AK21, (15.13), (15.15)]

(*i*) *The dimension of R is the same as the maximum cardinality of a set of elements of R that is algebraically independent over k.* [Hoc17, p. 59]

(*ii*) *If $P \subseteq Q$ are primes of R, all saturated chains of primes from P to Q have the same length.*

(*iii*) *Suppose that R is a domain. Then, all saturated chains from (0) to a prime ideal P have length equal to $\operatorname{ht}(P)$, and all saturated chains from P to a maximal ideal have length equal to $\dim(R/P)$. Moreover, we have*

$$\operatorname{ht}(P) + \dim(R/P) = \dim(R). \tag{5.7.3}$$

For every pair of prime ideals $P \subseteq Q$, every saturated chain from P to Q has length $\operatorname{ht}(Q) - \operatorname{ht}(P)$.

[AK21, (15.14)]

The condition in (*ii*) is called *catenary* [EGAIV$_1$, Chapitre 0, Proposition 14.3.2]. The formula (5.7.3) is from [EGAIV$_1$, Chapitre 0, Corollaire 14.3.5], and is called the *dimension formula* in [Hei17, Proposition 4.1] and [Har77, Chapter I, Theorem 1.8A(b)]. The dimension formula is also related to Nagata's altitude formula [Nag75, pp. 129–130].

Proof. We first show (*iii*). Choose any saturated chain from (0) to P of length r and choose a saturated chain from P to a maximal ideal $\mathfrak{m} \subseteq R$. The latter chain corresponds to a saturated chain in R/P, and hence has length $\dim(R/P)$. Putting these chains together gives a chain of length $r + \dim(R/P)$, which has length $\dim(R)$ by Theorem 5.5.2(*iii*). Thus, all saturated chains from (0) to P have length $\dim(R) - \dim(R/P)$, which must be the same as the height of P. The last statement about chains between prime ideals P and Q follows since a saturated chain from P to Q corresponds to a saturated chain from (0) to Q/P in R/P, which has length

$$\dim(R/P) - \dim\left(\frac{R/P}{Q/P}\right) = \dim(R/P) - \dim(R/Q),$$

which can be rewritten as

$$\big(\dim(R) - \operatorname{ht}(P)\big) - \big(\dim(R) - \operatorname{ht}(Q)\big) = \operatorname{ht}(Q) - \operatorname{ht}(P).$$

(*ii*) follows from (*iii*) since a saturated chain from P to Q corresponds to a saturated chain from (0) to Q/P in R/P.

To show (*i*), we note that there are at least $d = \dim(R)$ such algebraically independent elements by Noether's Normalization Theorem 5.2.5. Conversely, suppose that $k[x_1, x_2, \ldots, x_h] \subseteq R$, where $x_1, x_2, \ldots, x_h$ are algebraically independent. The set

$$W = k[x_1, x_2, \ldots, x_h] - \{0\}$$

is multiplicative in R and does not contain 0, and hence there is a prime ideal $P \subseteq R$ disjoint from W by Zorn's lemma (Proposition 1.5.5). We then have

$$P \cap k[x_1, x_2, \ldots, x_h] = (0),$$

which implies that the composition

$$k[x_1, x_2, \ldots, x_h] \hookrightarrow R \twoheadrightarrow R/P$$

is injective. We then have

$$d = \dim(R) \geq \dim(R/P) = \operatorname{trdeg}_k\big(\operatorname{Frac}(R/P)\big) \geq h,$$

since $\operatorname{Frac}(k[x_1, x_2, \ldots, x_h]) \subseteq \operatorname{Frac}(R/P)$. □

We end this section with an example where the dimension formula (5.7.3) fails. This is a higher-dimensional analogue of Example 5.7.1.

Example 5.7.4 [Hei17, Example 4.2]. Consider the ring

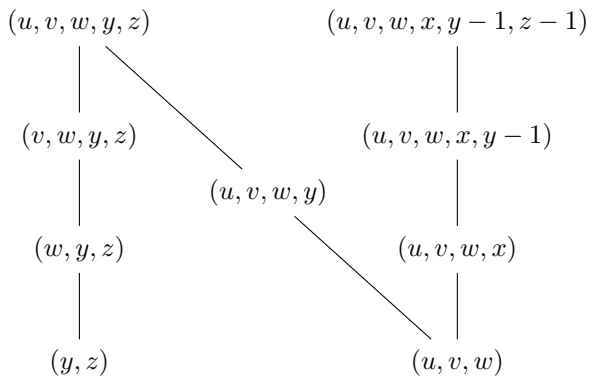
$$B = \frac{k[u, v, w, x, y, z]}{(uy, uz, vy, vz, wy, wz)}.$$

Since $(uy, uz, vy, vz, wy, wz) = (y, z) \cap (u, v, w)$, we can think of $\operatorname{MaxSpec}(B)$ geometrically as the union of k^4 and k^3 in k^6 along a line.

We now consider the localization

$$A = \Big(B - \big((u, v, w, y, z) \cup (u, v, w, x, y - 1, z - 1)\big)\Big)^{-1} B.$$

The ring is semi-local with maximal ideals corresponding to (u, v, w, y, z) and $(u, v, w, x, y - 1, z - 1)$, which are both of height 3, hence $\dim(A) = 3$ with both maximal ideals of height 3. We then have the following diagram of inclusions of prime ideals in A:



This ring still satisfies the conclusion of Theorem 5.7.2(*ii*) by Proposition 3.2.10, but does not satisfy the dimension formula (5.7.3) since setting $P = (u, v, w, y)$, we have

$$\mathrm{ht}(P) + \dim(A/P) = 1 + 1 = 2 < 3 = \dim(A).$$

CHAPTER 6

Chain conditions

We now want to define classes of rings and modules that we think of as having sufficiently strong finiteness properties to make them well-behaved.

6.1. Chain conditions in general

We start with the following very general definition.

DEFINITION 6.1.1. A partially ordered set $(P, \leq)$ is said to satisfy the *ascending chain condition* or *ACC* if, equivalently: [AK21, (16.3)] [Rei95, (3.1)] [Hoc17, p. 61] [AM69, p. 74]

(1) Every strictly ascending chain is finite.
(2) Every infinite non-decreasing chain is eventually constant.
(3) Every non-empty subset has a maximal element.

The implication (2) ⇒ (1) is clear, and (1) ⇒ (2) follows by removing redundant terms. The implication (3) ⇒ (1) follows since an infinite strictly ascending chain has no maximal element. The converse is more subtle, and uses the axiom of choice: If one has a non-empty subset with non maximal element, one can construct a strictly ascending sequence recursively.

Similarly, we have:

DEFINITION 6.1.2. A partially ordered set $(P, \leq)$ is said to satisfy the *descending chain condition* or *DCC* if, equivalently: [AK21, (16.26)] [Rei95, p. 51] [Hoc17, p. 61] [AM69, p. 74]

(1) Every strictly descending chain is finite.
(2) Every infinite non-increasing chain is eventually constant.
(3) Every non-empty subset has a minimal element.

6.2. Chain conditions for rings and modules

We now apply chain conditions to rings and modules by considering ideals and submodules, respectively, partially ordered by inclusion. 9/25

DEFINITION 6.2.1. A module M over a ring R is *Noetherian* (resp. *Artinian*) if it is the partially ordered set of submodules in M satisfies ACC (resp. DCC). We say that R itself is *Noetherian* (resp. *Artinian*) if it is Noetherian (resp. Artinian) as a module over itself. [AK21, (16.13)] [Rei95, p. 52] [Hoc17, p. 61] [AM69, p. 74]

These are named after Emmy Noether and Emil Artin, respectively. We note that the condition for a ring R to be Noetherian (resp. Artinian) is that the set of ideals in R satisfies ACC (resp. DCC).

EXAMPLE 6.2.2. We give some examples of Noetherian and Artinian modules. [AM69, pp. 74–76]

(1) Finite Abelian groups are both Noetherian and Artinian as $\mathbf{Z}$-modules.

(2) Fields k are both Noetherian and Artinian as rings: the only ideals are (0) and the entire field k.

[AK21, (16.1)] (3) The ring $\mathbf{Z}$ is Noetherian, but not Artinian. To see it is Noetherian, we note that $\mathbf{Z}$ is a PID, and hence a chain of ideals can be written as

$$(a_1) \subseteq (a_2) \subseteq \cdots .$$

For this to occur, we would need $a_j \mid a_i$ for every $j \geq i$. Since for fixed a_1, there can only be finitely many possibilities for a_j (using prime factorization), we see that the chain eventually stabilizes.

On the other hand, $\mathbf{Z}$ is not Artinian since for fixed $0 \neq a \in \mathbf{Z}$, the chain

$$(a) \supsetneq (a^2) \supsetneq \cdots$$

does not stabilize.

A similar argument works for $k[x]$. Our goal for much of today is to prove that this is indeed the case for polynomial rings in finitely many variables.

[AK21, (16.1)] [Rei95, (3.3)(1)] [Rei95, (3.3)(1)] (4) The polynomial ring $k[x_1, x_2, \ldots]$ in infinitely many variables is not Noetherian or Artinian because of the chains

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots ,$$
$$(x_1) \supsetneq (x_1^2) \supseteq \cdots .$$

(5) The property of being a Noetherian or Artinian ring does not necessarily pass to subrings. A simple way to see this is by taking a non-Noetherian or non-Artinian domain, and considering its embedding in its fraction field.

[AK21, (16.6)] [Rei95, (3.3)(3)] [Har77, Exer. II.4.12(b)(3)] Another example of a non-Noetherian ring is

$$k[x, y, x/y, x/y^2, x/y^3, \ldots] \subseteq k[x, y, y^{-1}].$$

Then, $(x) \subsetneq (x/y) \subsetneq (x/y^2) \subsetneq \cdots$ gives an infinite ascending chain. (Incidentally, the localization of this ring at (x, y) is a discrete rank *two* valuation ring.)

[AK21, (22.1)] [Rei95, Exer. 0.12] [Hoc17, p. 77] [AM69, p. 105] (6) Let $\mathbf{Z}_p \coloneqq \mathbf{Z}[\![x]\!]/(x - p)$ be the ring of *p-adic integers* for a prime $p > 0$. This is a DVR with maximal ideal (p), and we will see later today that it is Noetherian. You can think of this ring as formal power series in p: for example, $1 - p$ has inverse

$$1 + p + p^2 + \cdots$$

by the usual formula for geometric series. The ring

$$\mathbf{Z}_p[p^{1/p^\infty}]$$

obtained by adjoining all p-power roots of $\mathbf{Z}_p$ is very close to being an example of a *perfectoid* ring. Scholze's theory relates this to the ring

$$\mathbf{F}_p[\![t]\!][t^{1/p^\infty}].$$

Neither ring is Noetherian since there are ascending chains where you take principal ideals generated by p^e-power roots as $e \to \infty$.

Because we are ultimately more interested in Noetherian rings and modules, we will focus on these more.

We start with some equivalent characterizations of Noetherian modules.

[AK21, (16.13)]
[Hoc17, p. 62]
[AM69, Prop. 6.2]

PROPOSITION 6.2.3. *Let R be a ring, and consider an R-module M. The following are equivalent:*

(*i*) *M has ACC, i.e., M is Noetherian.*
(*ii*) *Every nonempty family of submodules of M has a maximal element.*
(*iii*) *Given any set S of elements of M spanning a submodule N of M, there is a finite subset of S spanning N.*
(*iv*) *Given any infinite sequence of elements of M spanning a submodule N, some finite initial segment of the sequence spans N.*
(*v*) *Every submodule of M is finitely generated.*

Proof. We already saw (*i*) $\Leftrightarrow$ (*ii*) in Definition 6.1.1.

To show (*ii*) $\Rightarrow$ (*iii*), we consider the family of submodules

$$\{N_0 \subseteq N \mid N_0 \text{ is generated by a finite subset } S_0 \subseteq S\},$$

where the empty subset spans 0 by convention. We claim that if N_0 is maximal in this set, then $N_0 = N$. It suffices to show that every element $s \in N$ in fact lies in N_0. But we have $N_0 \subseteq N_0 + R \cdot s \subseteq N$, and maximality implies that $N_0 = N_0 + R \cdot s \subseteq N$.

(*iii*) $\Rightarrow$ (*iv*) is clear since any finite subset of the sequence is contained in some finite initial segment of the sequence.

For (*iv*) $\Rightarrow$ (*v*), we show the contrapositive. Let $N \subseteq M$ be a submodule that is not finitely generated. We construct an infinite sequence as follows: Choose a nonzero element $n_1 \in N$. If $u_1, u_2, \ldots, u_n$ are chosen so that for every $i \in \{2, 3, \ldots, n\}$, the element u_i is not in the span of $u_1, u_2, \ldots, u_{i-1}$, note that since $R \cdot u_1 + \cdots + R \cdot u_n = N_n \subsetneq N$, we can choose $u_{n+1} \in N - N_n$. This sequence does not satisfy the condition in (*iv*).

Finally, to show (*v*) $\Rightarrow$ (*i*), if M has a non-decreasing chain of submodules N_i, then since their union N is finitely generated, eventually N_i contains all the generators of N, in which case the sequence is constant from thereon. □

EXAMPLE 6.2.4. We note that (*v*) is often the easiest condition to think about in practice. For example, this implies that

(1) All PID's (in particular, DVR's) are Noetherian. [AK21, (16.1)]
(2) All quotients and localizations of Noetherian rings are Noetherian (one can also see this using the correspondences of ideals from before in Propositions 1.3.12 and 3.2.10). [AK21, (16.7)] [AM69, Prop. 6.6]

We will also need to know how the Noetherian and Artinian conditions behave under short exact sequences. Below, for a short exact sequence $0 \to N \to M \to Q \to 0$, we will identify N with its image in M and Q with M/N to simplify notation.

LEMMA 6.2.5. *Let $0 \to N \to M \to Q \to 0$ be a short exact sequence of modules over a ring R.* [AK21, (16.14), (16.16), (16.17), (16.27)] [Rei95, p. 53] [Hoc17, p. 62] [AM69, Prop. 6.3, Cor. 6.4]

(*i*) *Let $M_0 \subseteq M_1 \subseteq M$ be a sequence of R-module inclusions, and suppose that $M_1 \cap N = M_0 \cap N$ and that the images of M_0 and M_1 in Q are the same. Then, $M_0 = M_1$.*
(*ii*) *M is Noetherian if and only if both N and Q are.*
(*iii*) *M is Artinian if and only if both N and Q are.*
(*iv*) *A finite direct sum of Noetherian (resp. Artinian) modules is Noetherian (resp. Artinian).*

In particular, over a fixed ring R, the property of a module being Noetherian is preserved under taking submodules or quotient modules.

Proof. For (*i*), consider $u \in M_1$. Then, some element $v \in M_0$ has the same image as u in Q. We therefore see that $v - u = w$ maps to 0 in Q, and hence $w \in M_1 \cap N = M_0 \cap N$. Thus, $u = v - w \in M_0$ as required.

For (*ii*), we first show $\Rightarrow$. An increasing chain in N is an increasing chain in M, and hence N is Noetherian. The inverse images in M of modules forming an increasing chain in Q form an increasing chain in M, and hence Q is Noetherian. For $\Leftarrow$, suppose we have an increasing chain in M. Then, the intersection of these modules with N are eventually constant, and the images of these modules in Q are eventually constant as well. (*i*) implies that the chain in M is eventually constant.

(*iii*) follows in the same way as in (*ii*) with the word "increasing" replaced by "decreasing."

(*iv*) follows from (*ii*) and (*iii*) by induction and using the short exact sequences $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$. □

[AK21, (16.15)]
[Hoc17, p. 63]

Remark 6.2.6. In Lemma 6.2.5(*i*), the hypothesis $M_0 \subseteq M_1$ is needed. Without this assumption, we can construct a counterexample as follows. Let k be an infinite field, and consider

$$0 \longrightarrow k \xrightarrow{\alpha} k^2 \xrightarrow{\beta} k \longrightarrow 0,$$

where the first map is $a \mapsto (a, 0)$ and the second map is $(a, b) \mapsto b$. For every $\lambda \in k - \{0\}$, the spans M_λ of $(1, \lambda)$ in $k \oplus k$ are mutually distinct lines in k^2. On the other hand, $\alpha^{-1}(M_\lambda) = 0$ and $\beta(M_\lambda) = k$ for every λ.

Over Noetherian rings, Noetherian modules have a particularly nice description.

[AK21, (16.19)]
[Hoc17, p. 63]
[AM69, Prop. 6.5]

Proposition 6.2.7. *A module M over a Noetherian ring R is Noetherian if and only if it is finitely generated. A module M over a ring R is Noetherian if and only if it is finitely generated and $R/\mathrm{Ann}_R(M)$ is a Noetherian ring.*

Proof. For the first statement, $\Leftarrow$ follows from Lemma 6.2.5: if R is Noetherian, then so is every finitely generated free module, and hence so is every finitely generated R-module. For the second statement, $\Leftarrow$ follows by considering M as a module over the ring $R/\mathrm{Ann}_R(M)$.

We now prove $\Rightarrow$. Suppose M is Noetherian. Then, M is finitely generated by Proposition 6.2.3. Now to show that $R/\mathrm{Ann}_R(M)$ is Noetherian, we will embed $R/\mathrm{Ann}_R(M)$ into the $R/\mathrm{Ann}_R(M)$-module M. Choose a finite set of generators $m_1, m_2, \ldots, m_n$ for M. We then consider the R-module map

$$\begin{aligned} R &\longrightarrow M^{\oplus n} \\ r &\longmapsto (rm_1, rm_2, \ldots, rm_n) \end{aligned}$$

An element $r \in R$ is in the kernel of this map if and only if it annihilates every generator of M, which is equivalent to being in the annihilator of M. Thus, there is an injection

$$\frac{R}{\mathrm{Ann}_R(M)} \hookrightarrow M^{\oplus n},$$

which we see is an injection of $R/\mathrm{Ann}_R(M)$-modules, and hence $R/\mathrm{Ann}_R(M)$ is Noetherian by Lemma 6.2.5, (*ii*) and (*iv*). □

6.3. Hilbert's basis theorem

We now want to show that polynomial rings are Noetherian. To do this, we first observe the following:

LEMMA 6.3.1. *Let R be a Noetherian ring. If S is a module-finite extension of R, then every subextension $R \subseteq B \subseteq S$ is module-finite over R, and is a Noetherian ring.* [Hoc17, p. 63]

Altman and Kleiman prove a more general statement due to Artin and Tate [AK21, (16.21)].

Proof. S is a Noetherian R-module. Since B is an R-submodule of S, we see that B is also finitely generated, and hence is Noetherian as an R-module. Finally, since any ideal of B is an R-submodule of B, the fact that B has ACC for R-modules implies that it has ACC for ideals (alternatively, any finite R-generating set for an ideal in B is also a B-generating set). □

We can now prove Hilbert's basis theorem, which states that polynomial rings are Noetherian. We give two proofs. The first is not standard, but shows that working over a field is nice because we have tools like the Noether normalization theorem.

THEOREM 6.3.2 (Hilbert's basis theorem over fields [Hil1890]). *The polynomial ring R in n variables over a field k is Noetherian. Hence, every finitely generated k-algebra is Noetherian.* [Hoc17, p. 64]

Proof. The second statement follows from the first as observed in Example 6.2.4(2), since any finitely generated k-algebra is a quotient of a polynomial ring in finitely many variables.

For $R = k[x_1, x_2, \ldots, x_n]$, we proceed by induction on n. The case $n = 0$ follows since $R = k$ is a field. Let I be a nonzero ideal of R and consider $f \in I - \{0\}$. To show that I is finitely generated, it suffices to show that $I/(f)$ is finitely generated in $R/(f)$, since if the images of $g_1, g_2, \ldots, g_s$ generate $I/(f)$ in $R/(f)$, then $g_1, g_2, \ldots, g_s, f$ generate I in R. After a change of coordinates (Lemma 5.2.3), we may assume that f is monic in x_n when viewed as an element of $k[x_1, \ldots, x_{n-1}][x_n]$, so that $R/(f)$ is module-finite over $k[x_1, \ldots, x_{n-1}]$. But this ring is Noetherian by inductive hypothesis, and hence $R/(f)$ is Noetherian by Lemma 6.3.1. □

We now show Hilbert's basis theorem in general. 9/27

THEOREM 6.3.3 (Hilbert's basis theorem). *Let R be a Noetherian ring. Then, every finitely generated R-algebra is Noetherian.* [AK21, (16.12)] [Rei95, (3.6)] [Hoc17, p. 64]

Proof. As before, it suffices to prove polynomial rings over R are Noetherian. Moreover, by inducing on the number of variables, it suffices to show that if R is Noetherian, then $R[x]$ is Noetherian.

Let $J \subseteq R[x]$ be an ideal. For $t \in \mathbf{N}$, let $I_t \subseteq R$ be the set of elements of R that occur as the leading coefficient of a polynomial of degree t in J, together with 0. Then, I_t is an ideal, and $I_t \subseteq I_{t+1}$ since the leading coefficient of xf is the same as that of f. Since R is Noetherian, we can choose m such that $I_m = I_{m+1} = \cdots$. For every $t \in \{0, 1, \ldots, m\}$, choose polynomials

$$f_{t,1}, \ldots, f_{t,h_t} \in J$$

of degree t whose leading coefficients generate I_t. We claim that the $f_{t,s}$ generate J. Let J_0 be the ideal they generate; we show that $J_0 = J$ by contradiction. Choose $g \in J - J_0$ of minimal degree. If g is of degree $t \leq s$, then we may subtract an R-linear combination j_0 of the $f_{t,s}$ (in which case $j_0 \in J_0$) that will cancel the leading term of g, and this will introduce no terms of degree larger than t. Since $g - j_0 \in J_0$ by minimality, we therefore have $g \in J_0$, a contradiction.

If the degree of g is $d > s$, then we can give the same argument by subtracting off an R-linear combination of the polynomials $x^{d-s} f_{m,s}$ to cancel the highest degree term. □

[Hoc17, p. 65]

COROLLARY 6.3.4. *A finitely generated algebra over a PID is Noetherian.*

Proof. Combine Example 6.2.4 and Hilbert's basis Theorem 6.3.3. □

6.4. Noetherian induction

There is a very useful trick for proving facts about Noetherian rings and modules, called Noetherian induction. The idea is as follows: If we want to prove a theorem about Notherian modules, suppose we have a counterexample M. Consider the family of submodules $N \subseteq M$ such that M/N is a counterexample. This family contains the 0 submodule, and so is non-empty, and has a maximal element. By working with M/N instead of M, we can now assume that every proper quotient of M satisfies the theorem. If R is a ring, these quotients R/I are also rings.

We illustrate this strategy in the following:

[Hoc17, p. 65]

THEOREM 6.4.1. *Every Noetherian ring has only finitely many minimal primes. Hence, every ideal of a Noetherian ring has only finitely many minimal primes containing it.*

Proof. The second statement follows from the first by passing to R/I, and hence it suffices to show the first. We proceed by Noetherian induction. We may assume that every proper quotient of R has only finitely many prime ideals. If R is a domain, then the only minimal prime is (0), and we are done. If R is not a domain, choose $x, y \in R - \{0\}$ such that $xy = 0$. Then, every minimal prime of R contains either x or y. If the former holds, it is a minimal prime of $R/(x)$, and there are only finitely many of these by the hypothesis of Noetherian induction. If the latter holds, it is a minimal prime of $R/(y)$, and we conclude as before. □

6.5. Examples of Artinian modules that are not Noetherian

Last time I was asked to give an example of an Artinian module that is not Noetherian. Here is one:

[AK21, (16.29)]
[AM69, pp. 74–75]

EXAMPLE 6.5.1. Let $p > 0$ be a prime number, and set

$$M \coloneqq H^1_{(p)}(\mathbf{Z}) \coloneqq \frac{\mathbf{Z}[1/p]}{\mathbf{Z}}.$$

We claim that M is Artinian but not Noetherian as a $\mathbf{Z}$-module.

We first show that if $N \subsetneq M$ is a proper submodule, then N is the submodule of M generated by $1/p^e$, where p^e is the largest denominator showing up for elements n/p^e for $p \nmid n$. If $n/p^e \in N$, then $1/p^e \in N$ since there exists $m \in \mathbf{Z}$ for which $mn \equiv 1 \bmod p^e$. Thus, either N contains all $1/p^e$, in which case $N = M$, or it does not, in which case there is a largest denominator p^e.

Now we note that M is Artinian since any chain of submodules looks like

$$\mathbf{Z} \cdot \frac{1}{p^{e_1}} \supseteq \mathbf{Z} \cdot \frac{1}{p^{e_2}} \supseteq \cdots$$

which corresponds to a descending chain of integers $e_1 \geq e_2 \geq \cdots$, which eventually stabilizes. On the other hand, M is not Noetherian since we have

$$\mathbf{Z} \cdot \frac{1}{p} \subsetneq \mathbf{Z} \cdot \frac{1}{p^2} \subsetneq \cdots .$$

A similar argument works for

$$H^1_{(x)}\big(k[x]\big) \coloneqq \frac{k[x, x^{-1}]}{k[x]}.$$

Here is another one:

Example 6.5.2 (Local cohomology). Let $R = k[x, y]$, and consider the map

$$\begin{aligned} \varphi\colon R_x \oplus R_y &\longrightarrow R_{xy} \\ \Big(\frac{r}{x^m}, \frac{s}{y^n}\Big) &\longmapsto \frac{ry^n - sx^m}{x^m y^n} \end{aligned}$$

The cokernel of φ is the second local cohomology module $H^2_{(x,y)}(R)$ of R with respect to the ideal (x, y).

We claim that $H^2_{(x,y)}(R)$ is Artinian but not Noetherian. The cokernel has the following k-vector space basis:

$$\begin{array}{ccccccc} & & & \dfrac{1}{xy} & & & \\ & & \dfrac{1}{x^2y} & & \dfrac{1}{xy^2} & & \\ & \dfrac{1}{x^3y} & & \dfrac{1}{x^2y^2} & & \dfrac{1}{xy^3} & \\ \iddots & & \vdots & & \vdots & & \ddots \end{array}$$

where multiplication by x moves up and to the right, and multiplication by y moves up and to the left. This module is not Noetherian since including more and more generators of the form $1/x^m y$, for example, gives an infinite strictly ascending chain. This module is Artinian: At least for submodules generated by a subset of the generators above, this is clear. The general case is easiest to prove using Matlis duality, although the version for $k[x]$ can be analyzed in a similar way to the previous example.

Remark 6.5.3. These modules are the best tool we know of to prove things similar to Open Problem 1.8.1. For example, the local cohomology module

$$H^3_{(xu,xv,yu,yv)}\big(k[x, y, u, v]\big) \neq 0$$

which can be used to show that (xu, xv, yu, yv) cannot be generated by two elements up to radical, and hence the union of two planes in k^4 described in Figure 5.1 cannot be defined by two equations.

We will see later that all Artinian rings are Noetherian.

6.6. More on algebraic sets

Now that we know that polynomial rings over fields, and more generally finitely generated algebras over fields, are Noetherian, we can say more about algebraic sets.

[Hoc17, p. 66]

LEMMA 6.6.1. *Let k be an algebraically closed field. For every algebraic set $Z(S) \subseteq k^n$, there exist finitely many elements $f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$ such that*

$$Z(S) = Z(f_1, f_2, \dots, f_m) = Z(f_1) \cap Z(f_2) \cap \cdots \cap Z(f_m).$$

Proof. We know that $Z(S) = Z(I)$, where I is the ideal generated by S. Since $k[x_1, x_2, \dots, x_n]$ is Noetherian by Hilbert's basis Theorem 6.3.3, there are finitely many elements $f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$ such that $I = (f_1, f_2, \dots, f_m)$. □

Thus, Hilbert's basis Theorem 6.3.3 allows us to apply our previous versions of Hilbert's Nullstellensatz (Theorem 5.3.3). Note that these results only applied to finitely generated ideals in $k[x_1, x_2, \dots, x_n]$!

To state this result, we need the following "inverse" to the map taking ideals to subsets of k^n.

DEFINITION 6.6.2. Let k be a field and let $X \subseteq k^n$ be a subset. The *ideal of X* is

$$I(X) \coloneqq \big\{ f \in k[x_1, x_2, \dots, x_n] \;\big|\; f(x) = 0 \text{ for all } x \in X \big\}.$$

The definition of $I(X)$ does not require k to be algebraically closed. For example, for k arbitrary, a point $P \coloneqq (\lambda_1, \lambda_2, \dots, \lambda_n) \in k^n$ satisfies

$$I\big(\{P\}\big) = (x_1 - \lambda_1, x_2 - \lambda_2, \dots, x_n - \lambda_n) =: \mathfrak{m}_P,$$

and

$$I(X) = \bigcap_{P \in X} \mathfrak{m}_P$$

is always a radical ideal. To apply the full strength of the Nullstellensatz (Theorem 5.3.3), however, we need the assumption that k is algebraically closed.

[Hoc17, p. 66]
[Har77, Cor. I.1.4]

THEOREM 6.6.3 (Hilbert's Nullstellensatz, second strong form). *Let k be an algebraically closed field. Consider the polynomial ring $R = k[x_1, x_2, \dots, x_n]$ and algebraic sets in k^n. There is a one-to-one inclusion-reversing correspondence*

$$\left\{ \begin{array}{c} \textit{algebraic sets} \\ \textit{in } k^n \end{array} \right\} \overset{\text{1-1}}{\longleftrightarrow} \left\{ \begin{array}{c} \textit{radical ideals} \\ \textit{in } R \end{array} \right\}$$

$$X \longmapsto I(X)$$

$$Z(I) \longmapsfrom I.$$

Proof. These two assignments are inclusion-reversing by definition, since for example, vanishing on a larger subset of k^n corresponds to more conditions on the ideal associated to that subset.

We first show that $I(Z(J)) = \sqrt{J}$ for arbitrary ideals $J \subseteq R$, which implies that $I(Z(I)) = I$ when I is a radical ideal. Since R is Noetherian by Hilbert's basis Theorem 6.3.3, we can write

$$J = (f_1, f_2, \dots, f_m)R.$$

We have

$$\begin{aligned} I\big(Z(J)\big) &= I\big(Z(f_1, f_2, \dots, f_m)\big) \\ &= \big\{ f \in R \,\big|\, f(P) = 0 \text{ for all } P \in Z(f_1, f_2, \dots, f_m) \big\} \\ &= \big\{ f \in R \,\big|\, f \in \sqrt{(f_1, f_2, \dots, f_m)} \big\} \\ &= \sqrt{J} \end{aligned}$$

where the third equality holds by the previous strong form of Hilbert's Nullstellensatz (Theorem 5.3.3).

It remains to show that $Z(I(X)) = X$ for an algebraic set $X \subseteq k^n$. Since X is an algebraic set, we have $X = Z(I)$ for an ideal I. Thus, we have

$$Z\big(I(X)\big) = Z\big(I\big(Z(I)\big)\big) = Z(\sqrt{I}) = X$$

since Hilbert's Nullstellensatz (Theorem 5.3.3) implies that $Z(I)$ only depends on I up to radical. Alternatively, use the corresponding fact for $\operatorname{Spec}(R)$ (Proposition 1.6.3) and the fact that $\operatorname{MaxSpec}(R)$ has the subspace topology (Corollary 5.3.1). □

6.7. Noetherian topological spaces

9/30

We now want to investigate geometric consequences of the Noetherian property. The first property is what corresponds to the finiteness of minimal primes we proved last time using Noetherian induction (Theorem 6.4.1). Recall that a nonempty closed set is *irreducible* if it cannot be written as a union of proper closed subsets (Definition 3.6.4).

We first write down a proof reducing back to the algebraic statement from before (Theorem 6.4.1), which says that Noetherian rings have finitely many minimal primes.

[Hoc17, p. 67]

Proposition 6.7.1. *Let R be a Noetherian ring. Every closed subset $Z \subseteq \operatorname{Spec}(R)$ has finitely many maximal closed irreducible subsets $Z_1, Z_2, \dots, Z_r$. We can then write*

$$Z = Z_1 \cup Z_2 \cup \cdots \cup Z_r$$

as the irredundant union of these maximal closed irreducible subsets, i.e., no one of the Z_i can be removed from this union. The maximal closed irreducible subsets of Z are the same as the maximal irreducible subsets of Z.

If k is an algebraically closed field, the same statements apply to algebraic sets in k^n.

Proof. The maximal irreducible closed subsets of Z correspond to the minimal prime ideals containing $I(Z)$ by Proposition 3.6.8. There are finitely many of these prime ideals P_i by Theorem 6.4.1. Moreover, since

$$I(Z) = \sqrt{I(Z)} = P_1 \cap P_2 \cap \cdots \cap P_r$$

by the Scheinnullstellensatz (Theorem 1.5.7), we see that

$$Z = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r),$$

and each of the $Z_i \coloneqq V(P_i)$ are irreducible by Proposition 3.6.8.

It remains to show that the Z_i are maximal and that no Z_i can be omitted from the union. Every irreducible subset $W \subseteq Z$ is contained in some Z_i since $W = \bigcup_i (W \cap Z_i)$ and hence $W = W \cap Z_i$ by the fact that W is irreducible. This

proves that the Z_i are maximal and that none of them could be omitted from the union: Otherwise, we would have $Z_j \subseteq \bigcup_{i \neq j} Z_i$, and hence $Z_j \subseteq Z_i$ for some i.

The case of algebraic sets in k^n is the same, replacing $V(-)$ with $Z(-)$. □

DEFINITION 6.7.2. Write $Z = Z_1 \cup Z_2 \cup \cdots \cup Z_r$ as in Proposition 6.7.1 for a closed subset $Z \subseteq \mathrm{Spec}(R)$ for R Noetherian or for $Z \subseteq k^n$. The Z_i are called the *irreducible components* of Z and the decomposition is called the *irreducible decomposition* of Z.

An *affine (algebraic) variety* is an irreducible closed subset of k^n, where k is an algebraically closed field. When talking about varieties, we often denote k^n by $\mathbf{A}_k^n$ to emphasize that we are not thinking of k^n as a vector space: isomorphisms of $\mathbf{A}_k^n$ are allowed to translate the origin to some other point.

One thing we want to point out is that the property of having irreducible decompositions can also be deduced as a consequence of the Noetherianity of the *space* $\mathrm{Spec}(R)$ or k^n.

[Hoc17, p. 68] DEFINITION 6.7.3. Let X be a topological space. We say that X is *Noetherian* if it satisfies DCC on closed sets.

Thus, if R is a Noetherian ring, then $\mathrm{Spec}(R)$ is Noetherian, and if k is an algebraically closed field, then k^n is Noetherian. We investigate this property more closely.

[Hoc17, p. 68] PROPOSITION 6.7.4. *Let X be a topological space.*

(*i*) *If X is Noetherian, then every subspace $Y \subseteq X$ is Noetherian.*
(*ii*) *If X is Noetherian, then X is quasi-compact.*
(*iii*) *X is Noetherian if and only if every open subspace is quasi-compact.*
(*iv*) *If X is Noetherian, then every closed subset Z is the finite irredundant union of its maximal irreducible closed subsets, which are the same as its maximal irreducible subsets.*

Proof. For (*i*), we note that if

$$Y_1 \supseteq Y_2 \supseteq \cdots$$

is a non-increasing sequence of closed subsets in Y, we can write $Y_i = Z_i \cap Y$ for some closed subset $Z_i \subseteq X$ for every i. The sequence

$$Z_1 \supseteq Z_1 \cap Z_2 \subseteq \cdots$$

is eventually stable in X, and the intersection at the n-th term with Y is

$$Y_1 \cap Y_2 \cap \cdots \cap Y_n = Y_n.$$

We now prove (*ii*). We show the "complement" version of quasi-compactness: If $\{Z_i\}$ is a family of subsets of X such that every finite subfamily has nonempty intersection, then $\bigcap_i Z_i$ is nonempty. By Noetherianity, the collection of intersections of finite subfamilies of the Z_i has a minimal element Z_0 that is nonempty by assumption. This Z_0 satisfies $Z_0 \subseteq Z_i$ for every i, for otherwise we could replace Z_0 by $Z_0 \cap Z_i$ to get a smaller intersection of finitely many Z_i. Thus, $\bigcap_i Z_i \supseteq Z_0 \neq \emptyset$.

We now prove (*iii*). The direction $\Rightarrow$ follows from combining (*i*) and (*ii*), and hence it suffices to show the converse. We show the contrapositive: If X is not Noetherian, then there exists a non-quasi-compact open subspace. Let

$$Z_1 \supsetneq Z_2 \supsetneq \cdots$$

be an infinite strictly decreasing sequence of closed subsets. Let $Z = \bigcap_i Z_i$. Then, $X - Z$ is open and is the strictly increasing union of the open sets $X - Z_i$. This gives an open cover of $X - Z$ with no finite subcover.

It remains to show (*iv*). We proceed by contradiction and use Noetherian induction as before. Consider the set of all possible counterexamples and let Z be a minimal counterexample. Then, Z cannot be irreducible, and hence $Z = Z_1 \cup Z_2$ for proper closed subsets $Z_1, Z_2 \subsetneq Z$. By minimality, Z_1 and Z_2 have irreducible decompositions. We can then omit terms until we have written Z as an irredundant finite union of irreducible closed subsets. The same argument as for Proposition 6.7.1 shows that if W is an irreducible subset of Z, then it is contained in one of the irreducible components of Z, and if W is maximal, then it is closed in Z and is an irreducible component of Z. □

We give some examples where thinking about rings geometrically and using irreducible decompositions can be useful when trying to understand rings.

EXAMPLES 6.7.5. Let k be an algebraically closed field. [Hoc17, pp. 67–68]

(*a*) Consider $Z(x_1x_2) = Z(x_1) \cup Z(x_2) \subseteq \mathbf{A}^2_k$. This represents the algebraic set $Z(x_1x_2)$ as the union of two axes, and this is an irredundant union of irreducible closed algebraic sets. This is the geometric interpretation of saying that $(x_1x_2) = (x_1) \cap (x_2)$ in $k[x_1, x_2]$.

(*b*) (A determinantal variety) Consider $\mathbf{A}^6_k$ with the coordinates $x_1, x_2, x_3, y_1, y_2, y_3$. We think of points in $\mathbf{A}^6_k$ as corresponding to 2×3 matrices with entries $x_1, x_2, x_3, y_1, y_2, y_3$:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}.$$

Let $\Delta_1 = x_2y_3 - x_3y_2$, $\Delta_2 = x_1y_3 - x_3y_1$, and $\Delta_3 = x_1y_2 - x_2y_1$ be the three 2×2 minors of this matrix.

Consider the algebraic set

$$Z(\Delta_2, \Delta_3) = \left\{ 2 \times 3 \text{ matrices} \;\middle|\; \begin{array}{c} \text{the minors formed from the first two columns} \\ \text{and the first and third columns vanish} \end{array} \right\}.$$

If $M \in Z(\Delta_2, \Delta_3)$, there are two possibilities. Either the first column is zero, or the first column is not zero. In the latter case, for the two minors to vanish, we know that the second and third columns are multiples of the first column, and hence Δ_1 also vanishes. From this, we see that

$$Z(\Delta_2, \Delta_3) = Z(x_1, y_1) \cup Z(\Delta_1, \Delta_2, \Delta_3).$$

This turns out to be an irreducible decomposition for $Z(\Delta_2, \Delta_3)$, although to show this, it remains to show that $Z(\Delta_1, \Delta_2, \Delta_3)$ is irreducible. This affine variety $Z(\Delta_1, \Delta_2, \Delta_3)$ is an example of a *determinantal variety* and the associated ring is a *determinantal ring*. See [BV88, Theorem 2.10] for one proof, and see [BV88, §2.E] for a discussion of the history behind this and other related results.

(*c*) (The cone over the projective twisted cubic curve) Consider $Z(\Delta_2, \Delta_3) \cap Z(x_2 - y_1, x_3 - y_2) \subseteq \mathbf{A}^6_k$. This set corresponds to matrices

$$\begin{pmatrix} w & x & y \\ x & y & z \end{pmatrix}$$

whose minors formed from the first two columns and the first and third columns vanish. The same analysis from above shows that

$$Z(\Delta_2, \Delta_3) \cap Z(x_2 - y_1, x_3 - y_2) \cong Z(w, x) \cup Z(wy - x^2, wz - xy, xz - y^2),$$

i.e., intersecting $Z(\Delta_2, \Delta_3)$ by the 4-plane $Z(x_2 - y_1, x_3 - y_2)$ yields the union of a 2-plane and the cone over the projective twisted cubic curve that you saw on Homework 1.

10/2

I wanted to show you another way to compute the kernel of the map defining the nodal cubic curve, since not all of you did it this way on Homework 5. This shows you how a lot of the material we have been working on comes together.

EXAMPLE 6.7.6. Let k be a field. Consider the k-algebra map

$$\begin{aligned} \varphi\colon k[x, y] &\longrightarrow k[t] \\ x &\longmapsto t^2 - 1 \\ y &\longmapsto t^3 - t. \end{aligned}$$

We want to show that $\ker(\varphi) = (y^2 - x^3 - x^2)$. The inclusion $\supseteq$ holds since

$$\begin{aligned} \varphi(y^2 - x^3 - x^2) &= (t^3 - t)^2 - (t^2 - 1)^2(t^2 - 1 + 1) \\ &= t^2(t^2 - 1)^2 - t^2(t^2 - 1) \\ &= 0. \end{aligned}$$

Conversely, we first note that $y^2 - x^3 - x^2$ is a prime element of $k[x, y]$. This is because one can apply Eisenstein's criterion to the prime ideal $(x + 1) \subseteq k[x]$, or alternatively one can apply Gauss's lemma and note that $y^2 - x^3 - x^2 \in k(x)[y]$ is irreducible since $x^2(x + 1)$ is not a square. Now note that $(0) \subsetneq (y^2 - x^3 - x^2)$, and hence $\operatorname{ht}(y^2 - x^3 - x^2) \geq 1$. On the other hand, $\operatorname{ht}(\ker(\varphi)) = 1$ by the dimension formula, since

$$\dim(\operatorname{im}(\varphi)) = \dim(k[t]) = 1$$

by the fact that $k[t^2 - 1, t^3 - t] \subseteq k[t]$ is an integral extension: $t = (t^3 - t)/(t^2 - 1)$ lies in the fraction field and satisfies $z^2 - (t^2 - 1 + 1)$.

6.8. The category of algebraic sets

Our next goal is to prove that when k is an algebraically closed field, the category of affine algebraic sets over k is equivalent to the category of reduced finite type k-algebras. This allows us to move back and forth between the two categories.

REMARK 6.8.1. For those of you also taking algebraic geometry, there are three differences between the presentation here and that in [Har77, Chapter 1, §§1–3]. First, the algebraic sets we are studying will be allowed to be reducible. Second, a related but distinct difference is that we will only consider *affine* algebraic sets, instead of trying to prove a statement about all morphisms from a quasi-projective variety X to an affine variety Y. Third, we will be a bit more careful about how to talk about regular functions on affine varieties. For example, one thing we did not prove in the algebraic geometry class is that the coordinate ring does not depend on the embedding of an algebraic set in $\mathbf{A}^n_k$, and that the assignment $X \mapsto k[X]$ is functorial with respect to these different choices. This sort of issue is one reason why working with $\operatorname{Spec}(R)$ and *schemes*, which are built by gluing spectra of rings together, ultimately leads to a nicer theory.

A last remark: You may wonder whether it is possible to build up a theory of "schemes" using only closed points, like we do with varieties over algebraically closed fields. The answer is that yes, such a theory is possible, as long as we restrict to a class of rings where a version of Hilbert's Nullstellensatz holds, called *Jacobson* rings. See [EGAI$_{\text{new}}$, Appendice].

We first turn the class of affine algebraic sets into a category by defining morphisms of affine algebraic sets.

DEFINITION 6.8.2. Let $X \subseteq \mathbf{A}_k^n$ and $Y \subseteq \mathbf{A}_k^m$ be (closed, affine) algebraic sets. A function $f\colon X \to Y$ is a *morphism* (sometimes called a *regular map*) of (affine) algebraic sets if there exist polynomials $g_1, g_2, \ldots, g_m \in k[x_1, x_2, \ldots, x_n]$ such that for all points $x \in X$, we have [Hoc17, pp. 68–69]

$$f(x) = \big(g_1(x), g_2(x), \ldots, g_m(x)\big).$$

Thus, f can be given by a polynomial formula in each of its coordinates.

Since the identity function is a morphism and the composition of morphisms is a morphism, we obtain a category whose objects are algebraic sets and whose morphisms are those defined above.

REMARK 6.8.3. One seemingly strange aspect of the definition is that we require a representation of f in terms of polynomials that come from the ambient space $\mathbf{A}_k^n$. This phenomenon is the algebraic analogue of the Tietze extension theorem from point-set topology. [Hoc17, p. 69]

We now turn to an important categorical aspect of this category of algebraic sets that allows us to move between the algebraic and geometric worlds. For those of you in the algebraic geometry class, this statement is a more general version of the affine case of the anti-equivalence of categories we proved in [Har77, §1.3].

DEFINITION 6.8.4. Let $X \subseteq \mathbf{A}_k^n$ be a closed algebraic set. The regular functions $X \to \mathbf{A}_k^1$ have the structure of a k-algebra: restrictions of polynomials g_1, g_2 to X have a sum (resp. a product) that is regular because it is the restriction of $g_1 + g_2$ (resp. $g_1 g_2$). This ring is called the *coordinate ring* of X and is denoted by $k[X]$. This ring is a reduced finitely type k-algebra: If a power of a function is 0, all of its values are nilpotent in k, and therefore 0 in k. The coordinate ring $k[X]$ is generated by the n functions represented by the variables $x_1, x_2, \ldots, x_n$, which assign to a point $x \in X$ its i-th coordinate. The functions in $x_1, x_2, \ldots, x_n$ are called the *coordinate functions* on $\mathbf{A}_k^n$ or X. The kernel of the map [Hoc17, pp. 69–70]

$$k[x_1, x_2, \ldots, x_n] \longrightarrow k[X]$$

is the ideal $I(X)$ of all polynomial functions that vanish on X.

The coordinate ring defines a representable functor

$$\begin{aligned} \mathcal{F}\colon \{\text{algebraic sets}\}^{\text{op}} &\longrightarrow \{\text{reduced finite type } k\text{-algebras}\} \\ X &\longmapsto k[X] \\ X &\longmapsto \operatorname{Hom}(X, \mathbf{A}_k^1). \end{aligned}$$

We define a representable functor in the opposite direction as follows:

$$\begin{aligned} \mathcal{G}\colon \{\text{reduced finite type } k\text{-algebras}\}^{\text{op}} &\longrightarrow \{\text{algebraic sets}\} \\ R &\longmapsto \operatorname{Hom}_{\mathsf{Alg}_k}(R, k). \end{aligned}$$

For this definition to make sense, we need to give $\mathrm{Hom}_{\mathsf{Alg}_k}(R,k)$ the structure of an algebraic set. To do so, let $r_1, r_2, \ldots, r_n \in R$ be a set of k-algebra generators. Then, we will show that we have an injection

$$\begin{aligned}\mathrm{Hom}_{\mathsf{Alg}_k}(R,k) &\longhookrightarrow \mathbf{A}_k^n \\ \phi &\longmapsto \big(\phi(r_1), \phi(r_2), \ldots, \phi(r_n)\big)\end{aligned}$$

with closed image, and that the resulting algebraic set does not depend on the generators $r_1, r_2, \ldots, r_n \in R$ up to isomorphism. This assignment makes $\mathcal{G}$ a contravariant functor by saying that if $h\colon R \to S$ is a k-algebra homomorphism, then the map

$$\begin{aligned}h^*\colon \mathrm{Hom}_{\mathsf{Alg}_k}(S,k) &\longrightarrow \mathrm{Hom}_{\mathsf{Alg}_k}(R,k) \\ \theta &\longmapsto \theta \circ h\end{aligned}$$

is given by composition.

Note that $\mathrm{Hom}_{\mathsf{Alg}_k}(R,k)$ is also in bijection with $\mathrm{MaxSpec}(R)$. Thus, our proof will show that $\mathrm{MaxSpec}(R)$ also has the structure of an algebraic set.

[Hoc17, p. 70]

THEOREM 6.8.5. *Let k be an algebraically closed field.*

(*i*) *Let R be a reduced finite type k-algebra. The procedure above gives $\mathrm{Hom}_{\mathsf{Alg}_k}(R,k)$ the structure of an algebraic set that does not depend on the generators $r_1, r_2, \ldots, r_n \in R$ (up to isomorphism).*

(*ii*) *$\mathcal{F}$ and $\mathcal{G}$ give an anti-equivalence of categories*

$$\{\textit{algebraic sets}\}^{\mathrm{op}} \underset{\mathcal{G}^{\mathrm{op}}}{\overset{\mathcal{F}}{\rightleftarrows}} \{\textit{reduced finite type } k\textit{-algebras}\}$$

Proof. (*i*). Let $r_1, r_2, \ldots, r_n$ be one set of generators of R. Consider the k-algebra map

$$\begin{aligned}k[x_1, x_2, \ldots, x_n] &\twoheadrightarrow R \\ x_i &\longmapsto r_i\end{aligned}$$

and let I be the kernel of this map, which is radical by the reducedness of R. Let us consider the map

$$\begin{aligned}\mathrm{Hom}_{\mathsf{Alg}_k}(R,k) &\longrightarrow \mathbf{A}_k^n \\ \phi &\longmapsto \big(\phi(r_1), \phi(r_2), \ldots, \phi(r_n)\big).\end{aligned}$$

This map is injective since each ϕ is uniquely determined by its values on the generators r_i. We now claim that the image is equal to $Z(I)$. This holds since a point $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ lies in the image if and only if the elements of I vanish on $(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

We now show that this structure as an algebraic set does not depend on the choice of generators $r_1, r_2, \ldots, r_n$. Let $r_1', r_2', \ldots, r_m'$ be another set of generators.

Then, we have the isomorphisms

$$\begin{array}{c} \bigcup_{\phi\in \mathrm{Hom}_{\mathsf{Alg}_k}(R,k)} \big\{\big(\phi(r_1),\phi(r_2),\ldots,\phi(r_n)\big)\big\} \\ \wr\uparrow\uparrow \\ \bigcup_{\phi\in \mathrm{Hom}_{\mathsf{Alg}_k}(R,k)} \big\{\big(\phi(r_1),\phi(r_2),\ldots,\phi(r_n),\phi(r'_1),\phi(r'_2),\ldots,\phi(r'_m)\big)\big\} \\ \wr\downarrow\downarrow \\ \bigcup_{\phi\in \mathrm{Hom}_{\mathsf{Alg}_k}(R,k)} \big\{\big(\phi(r'_1),\phi(r'_2),\ldots,\phi(r'_m)\big)\big\} \end{array}$$

given by the projection maps.

(*ii*). We first give a natural transformation

$$S\colon \mathrm{id} \Longrightarrow \mathcal{G}^{\mathrm{op}} \circ \mathcal{F}.$$

We need to show that we have commutative diagrams

$$\begin{array}{ccc} X & \xrightarrow{\qquad\theta\qquad} & Y \\ {\scriptstyle S_X}\downarrow & & \downarrow{\scriptstyle S_Y} \\ \mathrm{Hom}_{\mathsf{Alg}_k}\big(k[X],k\big) & \xrightarrow{(\mathcal{G}^{\mathrm{op}}\circ\mathcal{F})(\theta)} & \mathrm{Hom}_{\mathsf{Alg}_k}\big(k[Y],k\big). \end{array}$$

Let ϕ_x and ϕ'_y denote evaluation at $x \in X$ and $y \in Y$, respectively. Showing this square commutes is the same as showing

$$\big((\mathcal{G}^{\mathrm{op}} \circ \mathcal{F})(\theta)\big)(\phi_x) = \phi'_{\theta(x)}$$

for every $x \in X$. Now $\mathcal{F}(\theta)$ acting on $v \in k[Y]$ is $v \circ \theta$, and $\mathcal{G}^{\mathrm{op}}$ acts by composition as well. Thus,

$$\big((\mathcal{G}^{\mathrm{op}} \circ \mathcal{F})(\theta)\big)(\phi_x) = \big(v \mapsto v\big(\theta(x)\big)\big),$$

which is evaluation at $\theta(x)$. We now claim that S is an isomorphism of functors. To show this, we need to show that

$$S_X\colon X \longrightarrow \mathrm{Hom}_{\mathsf{Alg}_k}\big(k[X],k\big)$$

is an isomorphism. If we use the restricted coordinate functions on X as our generators for $k[X]$, this follows from the second strong version of Hilbert's Nullstellensatz (Theorem 6.6.3), which gives a bijection between $\mathrm{MaxSpec}(k[X])$ and the maximal ideals $\mathfrak{m}_y$ containing $I(X) \subseteq k[x_1, x_2, \ldots, x_n]$.

Finally, we need to show that $\mathcal{F}^{\mathrm{op}} \circ \mathcal{G}$ is isomorphic to the identity functor on finitely generated reduced k-algebras. We first give a natural transformation

$$T\colon \mathcal{F} \circ \mathcal{G}^{\mathrm{op}} \Longrightarrow \mathrm{id}.$$

We need to show that we have commutative diagrams

$$\begin{array}{ccc} R & \xrightarrow{\qquad\alpha\qquad} & S \\ {\scriptstyle T_R}\downarrow & & \downarrow{\scriptstyle T_S} \\ k\big[\mathrm{Hom}_{\mathsf{Alg}_k}(R,k)\big] & \xrightarrow{(\mathcal{F}^{\mathrm{op}}\circ\mathcal{G})(\alpha)} & k\big[\mathrm{Hom}_{\mathsf{Alg}_k}(S,k)\big]. \end{array}$$

The vertical map T_R is formed by mapping each element r to the function

$$f_r\colon \operatorname{Hom}_{\mathsf{Alg}_k}(R,k) \longrightarrow k$$

by the rule $f_r(u) = u(r)$, i.e., it is defined by evaluation. The commutative diagram commuting just means that evaluation in this way is natural in R: we get the maps

$$g_{\alpha(r)}(v) = v\big(\alpha(r)\big).$$

Finally, T_R is an isomorphism since writing $R \cong k[x_1, x_2, \ldots, x_n]/I$, then the isomorphism $k[Z(I)] \cong k[x_1, x_2, \ldots, x_n]/I$ follows from the second strong version of Hilbert's Nullstellensatz (Theorem 6.6.3). □

Definition 6.8.6. Given an algebraic set X over an algebraically closed field k, we can define $\dim(X) \coloneqq \dim(k[X])$, which equals the supremum of the dimensions of the irreducible components of X. The dimension at a point $x \in X$ is

$$\dim_x(X) \coloneqq \dim\big(k[X]_{\mathfrak{m}_x}\big) = \sup_{x \in X_i \text{ irr. comp.}} \big\{\dim(X_i)\big\}.$$

10/9

To recap, there are at least three ways to think about affine algebraic varieties X and their coordinate rings $k[X]$. The first is purely algebraic: we think of them as reduced finite type k-algebras.

The second is to consider X as a topological space associated to R. This is the point of view that leads to Grothendieck and Dieudonné's theory of schemes, where $\operatorname{MaxSpec}(R)$ is replaced by $\operatorname{Spec}(R)$. Even though the topic of this course is commutative algebra, this point of view is very important and useful in many algebraic applications!

The third comes from what we just proved. We saw that $\operatorname{Hom}_{\mathsf{Alg}_k}(R,k)$ was a useful set to look at, which gave another way to think about X. If S is *any* k-algebra, then this set $\operatorname{Hom}_{\mathsf{Alg}_k}(R,S)$ is in bijection with the set of solutions of the equations f_i generating $\ker(k[x_1,\ldots,x_n] \twoheadrightarrow R)$ in S^n. Thus, we can think of any k-algebra as encoding solutions to a system of equations. More generally, if S is any ring, then $\operatorname{Hom}(R,S)$ is the set of S-valued points. For X a scheme, the set to look at is the set of S-valued points $\operatorname{Hom}(\operatorname{Spec}(S), X)$. This leads to the point of view of the *functor of points*. This is the point of view of algebraic geometry that is most convenient for example when talking about algebraic groups, and came about later on in the development of scheme theory. It is possible to discuss all of algebraic geometry in this manner, but I do not recommend this for a first (or second?) course. See [DG70].

How does this point of view get used in practice? Let's see!

[Hoc17, pp. 73–74]

Example 6.8.7. Let

$$B = \frac{\mathbf{R}[X,Y,Z]}{(X^2+Y^2+Z^2-1)} =: \mathbf{R}[x,y,z]$$

and

$$S = \frac{B[U,V,W]}{(xU+yV+zW)} =: \mathbf{R}[x,y,z,u,v,w].$$

Then, the $\mathbf{R}$-valued points of B are

$$\operatorname{Hom}_{\mathsf{Alg}_{\mathbf{R}}}(B,\mathbf{R}) \longleftrightarrow \big\{(a,b,c) \in \mathbf{R}^3 \;\big|\; a^2+b^2+c^2 = 1\big\}$$

that is, the real 2-sphere of radius 1 centered at the origin in $\mathbf{R}^3$. The $\mathbf{R}$-valued points of S correspond to pairs $(a,b,c),(d,e,f)$ such that $(a,b,c) \in S^2$ and $(a,b,c)\cdot$

$(d, e, f) = 0$, i.e., (d, e, f) represents a tangent vector to the sphere at the point (a, b, c). Topologically, this means that the $\mathbf{R}$-valued points of S correspond to points of the tangent bundle to S^2.

Now a surprising fact is that $S[T] \cong B[T_1, T_2, T_3]$, but $S \ncong B[T_1, T_2]$! This boils down to the hedgehog theorem about how you cannot comb all the spines on a hedgehog flat without creating a cowlick. This answers a question I mentioned a while ago about cancelling variables, and is Hochster's original counterexample to the question [Hoc72a]. A key point in Hochster's proof is that even though this question is an algebraic one about polynomials, it is useful to construct examples using this functor of points point of view and some knowledge of topology.

6.9. Noether's theorem on rings of invariants

We end our chapter on chain conditions with two more results: Noether's theorem on rings of invariants and Hilbert's basis theorem for formal power series. [Hoc20a, p. 76]

Noether's theorem (due to Emmy Noether) was hugely influential in invariant theory. At the time, many people were trying to understand how different groups could act on k-algebras where k is a field. For the discussion below, fix a ring k and an k-algebra R. Recall that if G is a group, a *k-algebra action of G on R* is a group homomorphism

$$G \longrightarrow \mathrm{Aut}_{\mathsf{Alg}_k}(R),$$

that is, it is a way to multiply elements in R by elements in G compatibly with the group structure on G.

A reasonable question to ask is: If R is a finitely generated k-algebra and G acts by k-algebra automorphisms on R, is the *ring of invariants*

$$R^G \coloneqq \left\{ r \in R \;\middle|\; g(r) = r \text{ for all } g \in G \right\}$$

also a finitely generated k-algebra? A natural approach would be to try to write all the invariant elements down. However, Emmy Noether realized that one can prove finiteness properties without explicitly finding a set of generators. This proof motivated (in part) Noether's study of the Noetherian property.

Theorem 6.9.1 (Emmy Noether). *Let k be a Noetherian ring (for example, a field). Let R be a finitely generated k-algebra and let G be a finite group acting by k-algebra automorphisms on R. Then, the ring of invariants $R^G \subseteq R$ is finitely generated as a k-algebra, and is therefore Noetherian.*

Proof. Replacing k by its image in R, we may assume that $k \subseteq R$. Write

$$R = k[u_1, u_2, \ldots, u_n]$$

where the u_i are a finite set of generators (not necessarily algebraically independent) for R over k. Let $\{g_1, g_2, \ldots, g_s\}$ be the elements of G, where $s = |G|$. After permuting the g_j, we may assume that $g_1 = e \in G$.

For every i, an element $g \in G$ acts on the set of elements

$$g_1(u_i), g_2(u_i), \ldots, g_s(u_i)$$

by permutation. Thus, the elementary symmetric functions

$$\left\{ e_{i,j} \;\middle|\; 1 \le i \le n,\ 1 \le j \le s \right\}$$

are all in R^G. Consider the k-subalgebra

$$B \coloneqq k\left[e_{i,j} \middle| 1 \le i \le n,\ 1 \le j \le s \right] \subseteq R^G \subseteq R.$$

Then, B is finitely generated over k (as an algebra), and is therefore Noetherian by the Hilbert basis Theorem 6.3.3. We claim that every u_i is integral over B. First, u_i satisfies the equation

$$\prod_{j=1}^{s}(X - g_j(u_i)) = 0$$

since the first factor is $X - g_1(u_i) = X - u_i$. Moreover, the non-leading coefficients of this monic polynomial are the $e_{i,j}$ (up to a sign). Since the u_i generate R over k, they also generate R over B. It therefore follows that R is module-finite over B by Theorem 4.2.6, and is therefore Noetherian over B. Finally, since R^G is a B-submodule of R, we see that R^G is module-finite over B, and hence is finitely generated as a k-algebra. □

6.10. Hilbert's basis theorem for formal power series

We discussed a while ago how to form the ring of formal power series from an arbitrary ring R. There is a version of Hilbert's basis theorem for this process:

[Hoc17, p. 75] [AM69, p. 81]

THEOREM 6.10.1 (Hilbert's basis theorem for formal power series). *If R is a Noetherian ring then the formal power series ring $R[\![x_1, x_2, \ldots, x_n]\!]$ is Noetherian.*

The proof is very similar to the polynomial case in spirit, except we consider terms of *lowest* degree in the power series.

Proof. As before, by induction on n, it suffices to consider the case when $n = 1$. Let $J \subseteq R[\![x]\!]$ be an ideal. Let I_t be the set of elements $r \in R$ such that rx^t is the term of least degree in an element of J, together with 0. Again, this is an ideal in R. If $f \in J$ is not zero, and rx^t is the least degree term in f, then rx^{t+1} is the least degree term in $xf \in J$. This shows that $\{I_t\}_{t\geq 0}$ is a non-decreasing sequence of ideals in R. Since R is Noetherian, we may choose $k \in \mathbf{N}$ such that $I_k = I_{k+1} = \cdots$, and then for every $t \in \{0, 1, \ldots, k\}$ we can choose $f_{t,1}, \ldots, f_{t,h_t} \in J$ such that $f_{t,s}$ has smallest degree terms are $r_{t,s}x^t$ where $r_{t,1}, \ldots, r_{t,h_t}$ generate I_t.

As before, let J_0 be the ideal generated by the $f_{t,s}$. Let $u \in J$; we want to show that it lies in J_0. After replacing u by the result of subtracting off its lowest degree terms, we may assume that u has lowest degree term of degree $t \geq k$. We will in fact show:

CLAIM 6.10.2. *Let $u \in J$ such that its least degree term occurs in degree $t \geq k$. Then, $u \in (f_{k,1}, f_{k,2}, \ldots, f_{k,h_k})$.*

Note that this is a bit stronger than what we need. To simplify notation, we denote $f_s \coloneqq f_{k,s}$ and $h \coloneqq h_k$. We will do this by constructing partial sums for formal power series g_i such that $u = \sum_{i=1}^{h} g_i f_i$.

We will do this by constructing for every $i \in \{1, 2, \ldots, h\}$ and $m \in \mathbf{N}$ a sequence of polynomials $g_{i,m}(x) \in R[x]$ with the following properties:

(1) Every $g_{i,m}$ has degree at most m.
(2) If $m_1 < m_2$ then g_{i,m_1} is the sum of the terms of degree at most m_1 that occur in g_{i,m_2}. Given (1), this says that for all $m \geq 0$, we have $g_{i,m+1} - g_{i,m} = rx^{m+1}$ for some $r \in R$, which may be zero.
(3) For every m, the lowest degree term in $u - \sum_{i=1}^{h} g_{i,m} f_i$ has degree at least $k + m + 1$ (or this difference is zero).

The first two conditions imply that the $g_{i,m}$ are partial sums up to degree m of a formal power series.

To begin the induction, note that the lowest degree terms of u occurs in degree k or higher. Thus, the coefficient of x^k in u is in the ideal generated by the lowest degree coefficients of $f_1, \ldots, f_h$, and it follows that there are elements $r_{1,0}, \ldots, r_{h,0}$ of R such that the lowest degree term of $u - \sum_{i=1}^{h} r_{i,0} f_i$ occurs in degree at least $k+1$ (or is zero). We take $g_{i,0} = r_{i,0}$ for all i.

Now suppose the $g_{i,s}$ have been constructed for all $1 \leq i \leq h$ and $0 \leq s \leq m$. We now construct the $g_{i,m+1}$. Since $u' = u - \sum_{i=1}^{h} g_{i,m} f_i$ has lowest degree term of degree at least $m+k+1$, the coefficient of x^{m+k+1} is in the R-span of the coefficients of x^k in the f_i, and so we can choose $r_{i,m+1} \in R$ such that

$$u' - \sum_{i=1}^{h} r_{i,m+1} x^{m+1} f_i$$

has lowest degree term in degree at least $m+k+2$. It follows that if we take

$$g_{i,m+1} = g_{i,m} + r_{i,m+1} x^{m+1}$$

for $1 \leq i \leq h$, then (1) and (2) are satisfied, and (3) is as well since

$$u - \sum_{i=1}^{h} g_{i,m+1} f_i = u' - \sum_{i=1}^{h} r_{i,m+1} x^{m+1} f_i$$

has lowest degree term in degree at least $m+k+2$ (or is zero). For each i, let g_i be the formal power series whose partial sums are the $g_{i,m}$.

We finally need to show that $u = \sum_{i=1}^{h} g_i f_i$. To do so, it suffices to show that the coefficients of the corresponding powers of x are the same on both sides. Neither side has a nonzero term involving x^t for $t < k$. On the other hand, for all $m \geq 0$, the coefficient of x^{k+m} on the right will not change if we replace every g_i by $g_{i,m}$, since $g_i - g_{i,m}$ involves only terms of degree strictly larger than $m+k+1$. Thus, it suffices to show that for all $m \geq 0$, the difference

$$u - \sum_{i=1}^{h} g_{i,m} f_i$$

has coefficient zero on x^{m+k}, and this is true by (3). But then, $f_i \in J_0$, and hence $u \in J_0$. $\square$

CHAPTER 7

Tensor products and flatness

10/11

In this next part of the course, we will develop another operation on modules, called tensor products. One useful thing about this is that it gives a *extension of scalars* functor

$$\begin{aligned} \mathsf{Mod}_R &\longrightarrow \mathsf{Mod}_S \\ M &\longmapsto M \otimes_R S \end{aligned}$$

that is left adjoint to restriction of scalars.

7.1. Definition of tensor products

DEFINITION 7.1.1. Let R be a ring, and consider R-modules M, N, and W. An *R-bilinear map* $B\colon M \times N \to W$ is a function such that for every fixed $v \in N$, the map $B_v\colon M \to W$ defined by $B_v(u) = B(u,v)$ is R-linear, and the map $B^u\colon N \to W$ defined by $B^u(v) = B(u,v)$ is R-linear. The set of all R-bilinear maps $B\colon M \times N \to W$ is denoted $\mathrm{Bil}_R(M,N;W)$. [AK21, (8.1)] [Hoc17, p. 78]

The condition that a map $M \times N \to W$ is bilinear can be written concretely as follows: For all $u_1, u_2 \in M$, $v_1, v_2 \in N$, and $r_1, r_2, s_1, s_2 \in R$, we have

$$\begin{aligned} &B(r_1u_1 + r_2u_2, s_1v_1 + s_2v_2) \\ &\qquad = r_1s_1 \cdot B(u_1,v_1) + r_1s_2 \cdot B(u_1,v_2) + r_2s_1 \cdot B(u_2,v_1) + r_2s_2 \cdot B(u_2,v_2). \end{aligned}$$

EXAMPLE 7.1.2. The map [Hoc17, p. 78]

$$\begin{aligned} R \times R &\longrightarrow R \\ (r,r') &\longmapsto rr' \end{aligned}$$

is R-bilinear by the distributive property.

As before, we will construct the tensor product by hand and prove that it has a universal property. We actually state the universal property first this time:

THEOREM 7.1.3. *Let M and N be modules over a ring R. Then, there exists an R-module $M \otimes_R N$ together with a bilinear map $\beta\colon M \times N \to M \otimes_R N$ such that every R-bilinear map $B\colon M \times N \to W$ factors through $M \otimes_R N$:* [AK21, (8.3)] [Hoc17, p. 79] [AM69, Prop. 2.12]

$$\begin{array}{ccc} M \times N & \xrightarrow{\beta} & M \otimes_R N \\ & \searrow^{B} & \swarrow_{f}^{\exists!} \\ & W & \end{array}$$

CONSTRUCTION 7.1.4. Let M and N be R-modules. The *tensor product* of M [AK21, (8.2)] [Hoc17, p. 79] [AM69, p. 24]

and N is

$$M \otimes_R N \coloneqq \frac{R^{\oplus |M\times N|}}{\begin{pmatrix} b_{u+u',v} - b_{u,v} - b_{u',v} \\ b_{ru,v} - rb_{u,v} \\ b_{u,v+v'} - b_{u,v} - b_{u,v'} \\ b_{u,rv} - rb_{u,v} \end{pmatrix}}.$$

The map $\beta\colon M \times N \to M \otimes_R N$ is defined by sending (u, v) to the image of $b_{u,v}$, which we denote by $u \otimes v$.

[Hoc17, p. 78]

Remark 7.1.5. The construction of tensor products is not too important. The importance of tensor products really comes from the functor it represents:

$$\mathrm{Hom}_R(M \otimes_R N, W) \cong \mathrm{Bil}_R(M, N; W).$$

In other words, tensor products are the objects that turn bilinear maps into linear ones.

Proof of Theorem 7.1.3. To have $B = f \circ \beta$, we must have

$$f(u \otimes v) = f\big(\beta(u, v)\big) = B(u, v),$$

which shows that f is unique. To show it exists, define a map $f_0\colon R^{\oplus |M\times N|} \to W$ by $f_0(b_{u,v}) = B(u, v)$. This factors through $M \otimes_R N$ since it kills all the relations used in defining $M \otimes_R N$ by bilinearity. □

We note that in $M \otimes_R N$, we have the following relations:

(1) $(u + u') \otimes v = u \otimes v + u' \otimes v$;
(2) $u \otimes (v + v') = u \otimes v + u \otimes v'$;
(3) $(ru) \otimes v = r(u \otimes v) = u \otimes (rv)$.

We note some basic properties of tensor products.

[Hoc17, p. 79]
[AM69, Rem. (*i*) on p. 25, Prop. 2.16]

Proposition 7.1.6. *Let M and N be modules over a ring R. If M is generated by $\{u_i\}_{i\in I}$ and N is generated by $\{v_j\}_{j\in J}$, then $M \otimes_R N$ is generated by $\{u_i \otimes v_j\}_{i\in I, j\in J}$. In particular, if M and N are finitely generated R-modules, then $M \otimes_R N$ is finitely generated.*

Proof. Every element in $M \otimes_R N$ is an R-linear combination of elements $u \otimes v$ for $u \in M$ and $v \in N$. We therefore have

$$u \otimes v = \left(\sum_{s=1}^{m} r_s u_{i_s}\right) \otimes \left(\sum_{t=1}^{n} r'_t v_{j_t}\right) = \sum_{s,t} (r_s r'_t)(u_{i_s} \otimes v_{j_t}).$$ □

There are many things we can prove about tensor products using its universal property.

[Hoc17, p. 80]
[AM69, Prop. 2.14]

Proposition 7.1.7. *Let M, M', N, N' be modules over a ring R.*

(*i*) *(Commutative law) There is a unique isomorphism*

$$M \otimes_R N \xrightarrow{\sim} N \otimes_R M$$

mapping $u \otimes v$ to $v \otimes u$.

[AK21, (8.5)(1)]

[AK21, (8.5)(2)]

(*ii*) *(Unitary law) There is a unique isomorphism*

$$M \xrightarrow{\sim} R \otimes_R M$$

that maps u to $1 \otimes u$. The inverse maps $r \otimes u$ to ru.

[AK21, (8.4)]

(*iii*) *(Bifunctoriality) If* $f\colon M \to M'$ *and* $g\colon N \to N'$ *are* R*-linear, there is a unique* R*-linear map*

$$f \otimes g\colon M \otimes_R N \longrightarrow M' \otimes_R N'$$

such that $(f \otimes g)(u \otimes u') = f(u) \otimes g(u')$*. This gives rise to a functor*

$$\mathsf{Mod}_R \times \mathsf{Mod}_R \longrightarrow \mathsf{Mod}_R.$$

(*iv*) *(Distributive law) There is a unique isomorphism* [AK21, (8.11)]

$$(M \oplus M') \otimes_R N \xrightarrow{\sim} (M \otimes_R N) \oplus (M' \otimes_R N)$$

mapping $(u, u') \otimes v$ *to* $(u \otimes v, u' \otimes v)$*. This extends by induction to all finite direct sums, and to direct sums in the second factor.*

If $M = \bigoplus_{i \in I} M_i$ *and* $N = \bigoplus_{j \in J} N_j$ *are arbitrary direct sums, then*

$$M \otimes_R N \simeq \bigoplus_{(i,j) \in I \times J} M_i \otimes_R N_j.$$

(*v*) *If* F *is free over* R *on the free basis* $\{b_i\}_{i \in I}$*, and* F' *is free over* R *on the free basis* $\{b'_j\}_{j \in J}$*, then* $F \otimes_R F'$ *is free on the free basis* $\{b_i \otimes b'_j\}_{(i,j) \in I \times J}$*.*

Proof. (*i*) follows since $N \otimes_R M$ satisfies the universal property of $M \otimes_R N$: a bilinear map $B\colon M \times N \to W$ factors through $N \otimes_R M$ by considering the commutative diagram

$$\begin{array}{ccccc} M \times N & \xrightarrow{\sim} & N \times M & \longrightarrow & N \otimes_R M \\ & \searrow & & & \downarrow \exists! \\ & & & & W \end{array}$$

where we note that the composition $N \times M \to M \times N \to W$ is bilinear.

For (*ii*), we verify that the map $\beta\colon R \times M \to M$ sending (r, u) to ru satisfies the universal property. Given a bilinear map $B\colon R \times M \to W$, we define $f\colon M \to W$ by $m \mapsto B(1, m)$, which is linear since B is bilinear. Also,

$$B(r, u) = r \cdot B(1, u) = B(1, ru) = f(ru) = f(\beta(r, u)).$$

Furthermore, f is unique since β is surjective.

For (*iii*), the linear map is given by the universal property for the map $M \times N \to M' \otimes N'$ given by $(u, v) \mapsto f(u) \otimes g(v)$.

For (*iv*), there is a bilinear map $(M \otimes M') \times N \to (M \otimes N) \oplus (M' \otimes N)$ that sends $((u, u'), v) \mapsto (u \otimes v, u' \otimes v)$, which induces a map $(M \otimes M') \otimes_R N \to (M \otimes N) \oplus (M' \otimes N)$ by the universal property. In the other direction, By (*iii*), the injections $\iota\colon M \hookrightarrow M \oplus M'$ and $\iota'\colon M' \to M \oplus M'$ induce maps $\iota \otimes \mathrm{id}_N\colon M \otimes_R N \to (M \oplus M') \otimes_R N$ and $\iota' \otimes \mathrm{id}_N\colon M' \otimes_R N \to (M \oplus M') \otimes_R N$. These together give a map

$$(\iota \otimes \mathrm{id}_N) \oplus (\iota' \otimes \mathrm{id}_N)\colon (M \oplus M') \otimes_R N \longrightarrow (M \otimes_R N) \oplus (M' \otimes_R N).$$

You can check that these two maps are inverse to each other using elements of the form $(u, u') \otimes v$ on one side, and elements of the form $(u \otimes v, 0)$ and $(0, u' \otimes v)$ on the other.

For the infinite statement in (*iv*), we first consider the case when there is only one module N on the right. Consider any finite number of summands $M_{i_1}, \ldots, M_{i_n}$

on the left, and let M' be the direct sum of all the others. By (*iv*), we can write

$$M \otimes N \simeq \left(\bigoplus_{s=1}^{n} M_{i_s} \otimes_R N \right) \oplus (M' \otimes_R N).$$

It follows that every $M_i \otimes_R N$ injects into $M \otimes N$ as a direct summand, and that any one of them has intersection zero with a finite sum of the others. Since the M_i span M, the $M_i \otimes_R N$ span $M \otimes_R N$, and we therefore have the required direct sum decomposition. Replacing the roles of M and N, we get the desired decomposition.

Finally, (*v*) follows from the infinite statement in (*iv*) when $M_i = R$ and $N_j = R$ for every i and j, using (*ii*). □

7.2. Right exactness of tensor products and flatness

10/14

We now show that tensor products are right exact. Altman and Kleiman give a different proof using tensor–Hom adjunction [AK21, (8.11)], which I will mention again later.

[AK21, (8.11)]
[Hoc17, p. 81]
[AM69, Prop. 2.18]

Proposition 7.2.1 (Tensor products are right exact). *If $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an exact sequence of R-modules, then*

$$M' \otimes_R N \xrightarrow{f \otimes \mathrm{id}_N} M \otimes_R N \xrightarrow{g \otimes \mathrm{id}_N} M'' \otimes_R N \longrightarrow 0$$

is exact. We therefore have

$$M'' \otimes_R N \simeq \frac{M \otimes_R N}{(f \otimes \mathrm{id}_N)(M' \otimes_R N)},$$

i.e., tensor products preserve cokernels.

Proof. We will show that the map

$$g \otimes \mathrm{id}_N \colon M \otimes_R N \longrightarrow M'' \otimes_R N$$

is surjective with kernel $(f \otimes \mathrm{id}_N)(M' \otimes_R N)$. For surjectivity, we have that $M'' \otimes_R N$ is spanned by elements $u'' \otimes v$ for $u'' \in M''$ and $v \in N$, and it suffices to show that these elements are in the image of $g \otimes \mathrm{id}_N$. But by surjectivity of g, there exists $u \in M$ such that $g(u) = u''$, and hence $g(u \otimes v) = u'' \otimes v$.

We now note that $g \otimes \mathrm{id}_N$ induces a map

$$\frac{M \otimes_R N}{(f \otimes \mathrm{id}_N)(M' \otimes_R N)} \longrightarrow M'' \otimes_R N$$

by the fact the composition $M' \otimes_R N \to M'' \otimes_R N$ is zero. We construct an inverse h for this map as follows. First, we claim we can define a bilinear map

$$M'' \times N \longrightarrow \frac{M \otimes_R N}{(f \otimes \mathrm{id}_N)(M' \otimes_R N)}$$

mapping (u'', v) to (u, v), where $u \in M$ is an element such that $g(u) = u''$. We need to show that this assignment is independent of the choice of u. If u_1 also maps to u'', it differs from u by an element in the image of M', and hence

$$u \otimes v - u_1 \otimes v = (u - u_1) \otimes v \in f(M' \otimes_R N).$$

One can then check that this map is bilinear. The compositions of h and $g \otimes \mathrm{id}_N$ are the identity in either direction: it suffices to check this on pure tensors $[u \otimes v]$ or $g(u) \otimes v$, in which case this follows from definition. □

On the other hand, tensor products are not exact in general!

EXAMPLE 7.2.2. Consider the exact sequence [AK21, (8.12)] [Hoc17, pp. 81–82] [AM69, Ex. on p. 29]

$$0 \longrightarrow \mathbf{Z} \xrightarrow{2\cdot} \mathbf{Z} \longrightarrow \mathbf{Z}/(2) \longrightarrow 0$$

of $\mathbf{Z}$-modules, and apply $- \otimes_{\mathbf{Z}} \mathbf{Z}/(2)$. We then obtain

$$0 \longrightarrow \mathbf{Z}/(2) \xrightarrow{0} \mathbf{Z}/(2) \longrightarrow \mathbf{Z}/(2) \longrightarrow 0$$

which is not exact on the left-hand copy of $\mathbf{Z}/(2)$.

Note that the same example works for any nonzero element a in a domain A, in which case you consider

$$0 \longrightarrow A \xrightarrow{a\cdot} A \longrightarrow A/(a) \longrightarrow 0.$$

This motivates the following definition, which is due to Serre [GAGA, §21].

DEFINITION 7.2.3. We say that an R-module N is *flat* if $- \otimes_R N$ is exact. [AK21, (9.5)] [Hoc17, p. 87] [AM69, p. 29]

The right exactness above can be used to describe quotient modules in different ways.

COROLLARY 7.2.4. *If $M' \subseteq M$ and $N' \subseteq N$ are inclusions of R-modules, then* [Hoc17, p. 82]

$$\frac{M}{M'} \otimes_R \frac{N}{N'} \simeq \frac{M \otimes_R N}{\operatorname{im}(M \otimes_R N') + \operatorname{im}(M' \otimes_R N)}.$$

Proof. We have

$$\begin{aligned} \frac{M}{M'} \otimes_R \frac{N}{N'} &\simeq \frac{(M/M') \otimes_R N}{\operatorname{im}(M/M' \otimes_R N')} \\ &\simeq \frac{(M \otimes_R N)/\operatorname{im}(M' \otimes_R N)}{\operatorname{im}(M/M' \otimes_R N')}. \end{aligned}$$

The image of $M/M' \otimes_R N'$ in $(M \otimes_R N)/\operatorname{im}(M' \otimes_R N)$ is the image of $M \otimes_R N'$. □

COROLLARY 7.2.5. *Let R be a ring, and consider an R-module M and ideals $I, J \subseteq R$. Then, we have $(R/I) \otimes_R M \simeq M/IM$ and $(R/I) \otimes (R/J) \simeq R/(I+J)$.* [AK21, (8.14)] [Hoc17, p. 82]

Proof. This is on Homework 7. □ [AM69, Exer. 2.2]

7.3. Tensor products of multiple factors

One can extend the construction of tensor products to incorporate multiple factors.

DEFINITION 7.3.1. If $M_1, M_2, \ldots, M_k, W$ are R-modules, a map [AK21, p. 40] [Hoc17, p. 83] [AM69, p. 26]

$$M_1 \times M_2 \times \cdots \times M_k \longrightarrow W$$

is *k-multilinear* over R if, for every i, it becomes an R-linear function of u_i when all other entries $u_1, \ldots, u_{i-1}, u_{i+1} \ldots, u_k$ are fixed. When $k = 2$ this is the same as a bilinear map, and when $k = 3$, we say it is *trilinear*.

THEOREM 7.3.2 (Associativity of tensor products). *We have $(M_1 \otimes_R M_2) \otimes_R M_3 \simeq M_1 \otimes_R (M_2 \otimes_R M_3)$ for R-modules M_1, M_2, M_3.* [AK21, (8.9)] [Hoc17, pp. 83–84]

More generally, $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_k$ has meaning independent of how one inserts parentheses. [AM69, p. 26]

Proof. Both sides are universal for trilinear maps $M_1 \times M_2 \times M_3 \to W$. The second statement follows similarly by noting that all ways to insert parentheses are universal for k-multilinear maps $M_1 \times M_2 \times \cdots \times M_k \to W$. □

7.4. Extension of scalars

We now want to return to one of our original motivations, which was to give a way to go from R-modules to S-modules. We start with something a bit more general:

[AK21, (8.7)] [Hoc17, p. 84] [AM69, p. 28]

LEMMA 7.4.1. *Let M_1 be an S-module and let M_2 be an R-module, where R is a ring and S is an R-algebra. Then, $M_1 \otimes_R M_2$ has the structure of an S-module, where*

$$s(u_1 \otimes u_2) = (su_1) \otimes u_2.$$

The same statement holds reversing the roles of M_1 and M_2.

Proof. We have an R-trilinear map

$$S \times M_1 \times M_2 \longrightarrow M_1 \otimes_R M_2$$

sending (s, u_1, u_2) to $(su_1) \otimes u_2$. This gives an R-linear map

$$S \otimes_R (M_1 \otimes_R M_2) \longrightarrow M_1 \otimes_R M_2,$$

and hence an R-bilinear map

$$S \times (M_1 \otimes_R M_2) \longrightarrow M_1 \otimes_R M_2.$$

This is the map we use for multiplication by s, and has the formula claimed. The R-bilinearity implies almost all of the conditions needed to make $M_1 \otimes_R M_2$ into an S-module, except for the axiom that for all $z \in M_1 \otimes_R M_2$ and $s, s' \in S$, we have $(ss')z = s(s'z)$. Since multiplication by an element of S is R-linear, it suffices to check this for elements generating $M_1 \otimes_R M_2$ as an R-module. We can therefore assume $z = u_1 \otimes u_2$. But then,

$$(ss')(u_1 \otimes u_2) = \big((ss')u_1\big) \otimes u_2 = \big(s(s'u_1)\big) \otimes u_2 = s\big((s'u_1) \otimes u_2\big) = ss'(u_1 \otimes u_2). \quad \square$$

[Hoc17, p. 84]

REMARK 7.4.2. If M_1 and M_2 are both S-modules, then $M_1 \otimes_R M_2$ has two S-module structures coming from the left and from the right. These are almost always different, since when we tensor over R, scalars from S cannot be passed through the tensor symbol.

Using this S-module structure we have a slightly more general version of what we had before:

[AK21, (8.9)] [Hoc17, p. 84] [AM69, Exer. 2.15]

PROPOSITION 7.4.3. *Let $R \to S$ be a ring map. If M and N are S-modules and Q is an R-module, then*

$$(M \otimes_S N) \otimes_R Q \simeq M \otimes_S (N \otimes_R Q)$$

as S-modules, where $(u \otimes v) \otimes w$ corresponds to $u \otimes (v \otimes w)$.

Proof. We construct an isomorphism from left to right. For each $w \in Q$, there is an S-bilinear map $B_w \colon M \times N \to M \otimes_S (N \otimes_R Q)$ defined by $B_w(u, v) = u \otimes (v \otimes w)$. This gives an S-linear map

$$g_w \colon M \otimes N \longrightarrow M \otimes_S (N \otimes_R Q).$$

We can also define an R-bilinear map

$$(M \otimes_S N) \times Q \longrightarrow M \otimes_S (N \otimes_R Q)$$

by $(y, w) \mapsto g_w(y$, which induces an R-linear map

$$(M \otimes_S N) \otimes_R Q \longrightarrow M \otimes_S (N \otimes_R Q)$$

sending $(u \otimes v) \otimes w$ to $u \otimes (v \otimes w)$. This map turns out to be S-linear: we consider

$$s\big((u \otimes v) \otimes w\big) = (su \otimes v) \otimes w,$$

which has image

$$(su) \otimes (v \otimes w) = s\big(u \otimes (v \otimes w)\big).$$

To construct the inverse, fix $u \in M$ and define an R-bilinear map

$$B'_u \colon N \times Q \longrightarrow (M \otimes_S N) \otimes_R Q$$

by the rule $B'_u(v, w) = (u \otimes v) \otimes w$, which gives an R-linear map

$$g'_u \colon N \otimes_R M \longrightarrow (M \otimes_S N) \otimes_R Q.$$

This is S-linear since $(u \otimes sv) \otimes w = s(u \otimes (v \otimes w))$. We then define an S-bilinear map

$$M \times (N \otimes_R Q) \longrightarrow (M \otimes_S N) \otimes_R Q$$

sending (u, z) to $g'_u(z)$. We then have S-linear maps in both directions that on generators interchange $(u \otimes v) \otimes w$ and $u \otimes (v \otimes w)$. □

We can now define extension of scalars.

Definition 7.4.4. Let $R \to S$ be a ring map. We then have a covariant right exact functor [AK21, (8.7)] [Hoc17, p. 85] [AM69, p. 28]

$$\begin{aligned} \mathsf{Mod}_R &\longrightarrow \mathsf{Mod}_S \\ M &\longmapsto S \otimes_R M \\ f &\longmapsto \mathrm{id}_S \otimes f \end{aligned}$$

which we call *extension of scalars* or *base change*, because the "base ring" R is replaced by another base ring S.

Proposition 7.4.5 (Localization as extension of scalars). *Let R be a ring, and consider a localization $S = W^{-1}R$ of R. There is an S-isomorphism* [AK21, (12.13)] [Hoc17, p. 87] [AM69, Prop. 3.5]

$$f \colon S \otimes_R M \longrightarrow W^{-1}M$$

sending $(r/w) \otimes m$ to rm/w.

Proof. We have an R-bilinear map

$$S \times M \longrightarrow W^{-1}M$$

sending $((r/w), m) \mapsto rm/w$. This gives rise to a R-linear map

$$f \colon S \otimes_R M \longrightarrow W^{-1}M$$

This map is clearly surjective, and is S-linear since

$$\begin{aligned} s \cdot \Big(\sum_i \frac{r_i}{w_i} \otimes m_i\Big) &\longmapsto \sum_i s \cdot \frac{r_i m_i}{w_i} \\ \sum_i \Big(s \cdot \frac{r_i}{w_i}\Big) \otimes m_i &\longmapsto \sum_i s \cdot \frac{r_i m_i}{w_i} \end{aligned}$$

To check it is injective, consider an element

$$\sum_i \frac{r_i}{w_i} \otimes m_i.$$

We claim it is equal to an element of the form $(1/w) \otimes m$. Let $w = \prod_i w_i \in W$ and $v_i = \prod_{j \neq i} w_j \in W$. Then,

$$\sum_i \frac{r_i}{w_i} \otimes m_i = \sum_i \frac{r_i v_i}{w} \otimes m_i = \sum_i \frac{1}{w} \otimes r_i v_i m_i = \frac{1}{w} \otimes \sum_i r_i v_i m_i,$$

which is of the desired form.

We now check the map f is injective. Suppose $f((1/w) \otimes m) = 0$. Then, $m/w = 0$, and hence there exists $t \in W$ such that $tm = 0$. We therefore have

$$\frac{1}{w} \otimes m = \frac{t}{tw} \otimes m = \frac{1}{tw} \otimes tm = \frac{1}{tw} \otimes 0 = 0. \qquad \square$$

10/16

[AK21, (12.18)]
[Hoc17, p. 88]
[AM69, Cor. 3.6]

COROLLARY 7.4.6. *Let R be a ring. Then, every localization $W^{-1}R$ of R is flat as an R-module.*

Proof. This follows since we know localization is exact, and by the isomorphism given above. $\square$

7.5. Presentations and extension of scalars

To get a better feel for how extension of scalars works in examples, we want an explicit way to describe modules.

[AK21, (5.18)]
[Hoc17, pp. 85–86]

DEFINITION 7.5.1. Let M be a module over a ring R. A *presentation* for M is an exact sequence of the form

$$R^{\oplus J} \longrightarrow R^{\oplus I} \twoheadrightarrow M \longrightarrow 0,$$

where I and J are indexing sets. If both I and J are finite, we say that the presentation is *finite*. If M has a finite presentation, we say that M is *finitely presented*.

A map $R^{\oplus J} \to R^{\oplus I}$ defines a module M by taking the cokernel of the map. In practice, this is how you feed the data of a module to a computer.

Conversely, given M, a presentation can be constructed as follows: We first choose a set of generators $\{m_i\}_{i \in I}$ for M, and define the surjection $R^{\oplus I} \twoheadrightarrow M$ by sending the i-th generator of $R^{\oplus I}$ to m_i. Then, we do the same for the kernel of $R^{\oplus I} \twoheadrightarrow M$, in which case the resulting sequence is exact by definition. This process allows one to say the following:

[AK21, (16.19)]
[Hoc17, p. 86]

THEOREM 7.5.2. *Let R be a Noetherian ring. Then, for an R-module M, the following are equivalent:*

(*i*) *M is Noetherian.*
(*ii*) *M is finitely generated.*
(*iii*) *M is finitely presented.*

Proof. It suffices to show that if M is finitely generated, then it is finitely presented. Since M is finitely generated, there is a surjection $R^{\oplus m} \twoheadrightarrow M$ for finite m. Now $R^{\oplus m}$ is finitely generated, hence Noetherian, and therefore the kernel K of $R^{\oplus m} \twoheadrightarrow M$ is also finitely generated, and admits a surjection $R^{\oplus n} \twoheadrightarrow K$ giving rise to an exact sequence $R^{\oplus n} \to R^{\oplus m} \to M \to 0$. $\square$

When I and J are finite, we can represent the map $R^{\oplus J} \to R^{\oplus I}$ as a matrix with entries indexed by $I \times J$.

EXAMPLE 7.5.3.

(1) If M is the ideal $I = (x, y) \subseteq k[x, y] = R$, then a presentation is given by

$$R \xrightarrow{\left(\begin{smallmatrix} y \\ -x \end{smallmatrix}\right)} R^{\oplus 2} \xrightarrow{\left(\begin{smallmatrix} x & y \end{smallmatrix}\right)} I$$

This sequence is actually exact on the left, and hence gives an example of a *free resolution* for I.

(2) The example above was not too bad, since we could guess what the kernel was generated by. Our favorite example from Homework 1 is pretty subtle: letting $I = (xz - y^2, -wz + xy, wy - z^2) \subseteq k[w, x, y, z] = R$, the presentation is given by

$$R^{\oplus 2} \xrightarrow{\left(\begin{smallmatrix} w & x \\ x & y \\ y & z \end{smallmatrix}\right)} R^{\oplus 3} \xrightarrow{\left(\begin{smallmatrix} xz-y^2 & -wz+xy & wy-z^2 \end{smallmatrix}\right)} I$$

This one is also exact on the left.

Exactness on the left does not happen in general; for example, you could consider a presentation for R/I instead of I. Computing presentations like this is very difficult!

We now describe how extension of scalars acts on modules. Given a presentation

$$R^{\oplus J} \longrightarrow R^{\oplus I} \twoheadrightarrow M \longrightarrow 0,$$

the right exactness of $S \otimes_R -$ implies that

$$S^{\oplus J} \longrightarrow S^{\oplus I} \twoheadrightarrow S \otimes_R M \longrightarrow 0$$

is a presentation for $S \otimes_R M$, where we use the fact that tensor products commute with arbitrary direct sums. If I and J are finite, then the matrix defining $S^{\oplus J} \to S^{\oplus I}$ is obtained by applying the map $R \to S$ on each entry.

We also have:

Corollary 7.5.4. *Let $R \to S$ be a ring map. If M is a finitely generated (resp. finitely presented) R-module, then $S \otimes_R M$ is a finitely generated (resp. finitely presented) S-module.*

7.6. Tensor–Hom adjunction

Our goal now is to describe how tensor products and extension of scalars are related to other functors we have seen before.

Theorem 7.6.1. *Let $R \to S$ be a ring map, and consider an R-module M and S-modules N and P. Then, there is an R-module isomorphism* [AK21, (8.9)]

$$\sigma\colon \operatorname{Hom}_S(M \otimes_R N, P) \longrightarrow \operatorname{Hom}_R\big(M, \operatorname{Hom}_S(N, P)\big)$$

that is functorial in M, N, and P.

Proof. If $g\colon M \otimes_R N \to P$ is on the left-hand side, then we define

$$\big(\sigma(g)(u)\big)(v) = g(u \otimes v).$$

The map $\sigma(g)(u)$ is S-linear since for every $s \in S$, we have

$$\big(\sigma(g)(u)\big)(sv) = g(u \otimes sv) = s \cdot g(u \otimes v).$$

Furthermore, $\sigma(g)$ is R-linear, since for every $r \in R$, we have

$$\big(\sigma(g)(ru)\big)(v) = g(ru \otimes v) = g(u \otimes rv) = \big(\sigma(g)(u)\big)(rv).$$

The inverse

$$\theta\colon \operatorname{Hom}_R\big(M, \operatorname{Hom}_S(N,P)\big) \longrightarrow \operatorname{Hom}_S(M \otimes_R N, P)$$

is given by defining $B\colon M \times N \to P$ by $B(u,v) = (f(u))(v)$. This is R-bilinear. □

This immediately shows that tensor products are right-exact: they are left adjoints [AK21, (6.12)].

A while ago we asked whether localization is an adjoint functor. Given that localization is a special case of extension of scalars, the following shows that localization is the left adjoint to restriction of scalars along the localization map $R \to W^{-1}R$.

Corollary 7.6.2 (Extension of scalars and restriction of scalars are adjoint). [Hoc17, p. 86] *There is an R-module isomorphism*

$$\operatorname{Hom}_S(S \otimes_R M, P) \simeq \operatorname{Hom}_R(M, P)$$

that is functorial in M and N. Thus, $S \otimes_R M$ represents the functor $\operatorname{Hom}_R(M, -)$.

Proof. Apply Theorem 7.6.1 when $N = S$, using that $\operatorname{Hom}_S(S, N) \simeq N$. □

7.7. Left exactness of Hom

We also have:

Proposition 7.7.1. [AK21, (5.17)] [Hoc17, p. 89] [AM69, Prop. 2.9] *Let R be a ring, and consider an R-module N.*

(*i*) *Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be an exact sequence of R-modules over a ring R. Then,*

$$0 \longrightarrow \operatorname{Hom}_R(N, M') \longrightarrow \operatorname{Hom}_R(N, M) \longrightarrow \operatorname{Hom}_R(N, M'')$$

is an exact sequence, and hence $\operatorname{Hom}_R(N, -)$ defines a left exact covariant functor $\mathsf{Mod}_R \to \mathsf{Mod}_R$.

(*ii*) *Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be an exact sequence of R-modules. Then,*

$$0 \longrightarrow \operatorname{Hom}_R(M'', N) \longrightarrow \operatorname{Hom}_R(M, N) \longrightarrow \operatorname{Hom}_R(M', N)$$

is an exact sequence, and hence $\operatorname{Hom}_R(-, N)$ defines a left exact contravariant functor $\mathsf{Mod}_R^{\mathrm{op}} \to \mathsf{Mod}_R$.

Proof. For (*i*), exactness on the left follows since if $g\colon N \to M'$ is a nonzero map, then $\alpha \circ g\colon N \to M' \to M$ is also nonzero. Exactness in the middle follows since for $f\colon N \to M$, the composition $\beta \circ f\colon N \to M''$ is zero if and only if $f(v) \in M'$ for every $v \in N$, which holds if and only if f came from a map $N \to M'$.

For (*ii*), exactness on the left follows since if $f(u'') \neq 0$, then there exists $u \in M$ such that $\beta(u) = u''$, and hence $(f \circ \beta)(u) \neq 0$. Exactness in the middle follows since for $f\colon M \to N$, the composition $f \circ \alpha\colon M' \to N$ is zero if and only if $f|_{M'}\colon M' \to N$ is zero. But this holds if and only if f factors through M'', in which case this map $M'' \to N$ has image equal to f. □

The same example from before shows that right exactness does not hold in general.

[Hoc17, p. 89]

EXAMPLE 7.7.2. Consider the short exact sequence

$$0 \longrightarrow \mathbf{Z} \xrightarrow{2\cdot} \mathbf{Z} \longrightarrow \mathbf{Z}/(2) \longrightarrow 0.$$

Applying $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/(2), -)$ gives the left exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/(2), \mathbf{Z}) \xrightarrow{2\cdot} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/(2), \mathbf{Z}) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/(2), \mathbf{Z}/(2)).$$

But the modules on the left and middle are equal to zero. Similarly, applying $\mathrm{Hom}_{\mathbf{Z}}(-, \mathbf{Z})$, we obtain the left exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/(2), \mathbf{Z}) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z}) \xrightarrow{2\cdot} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}, \mathbf{Z})$$

and the module on the left is equal to zero. On the other hand, the map on the right is not surjective: it is the multiplication by 2 map on $\mathbf{Z}$.

Last time, we asked whether $M \otimes_R M \cong M$. This is not the case. 10/18

EXAMPLE 7.7.3. $k^{\oplus 2} \otimes_k k^{\oplus 2} \cong k^{\oplus 4} \ncong k^{\oplus 2}$.

Left exactness of Hom has the following nice consequence.

PROPOSITION 7.7.4 (Hom commutes with flat base change). *Let $R \to S$ be a ring map, and let M and N be R-modules. There is an S-linear map* [AK21, (9.18)] [Hoc17, p. 96]

$$\begin{aligned} \theta \colon S \otimes_R \mathrm{Hom}_R(M, N) &\longrightarrow \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\ s \otimes f &\longmapsto (s \cdot -) \otimes f \end{aligned}$$

that is functorial in M and N. If $R \to S$ is flat and M is finitely generated (resp. finitely presented), then θ is injective (resp. bijective).

An important special case to consider is when $S = W^{-1}R$.

Proof. The map $s \otimes f \mapsto (s \cdot -) \otimes f$ is R-linear since it is induced by the R-bilinear map $(s, f) \mapsto (s \cdot -) \otimes f$. It is moreover S-linear since $s'(s \otimes f) = (s's) \otimes f$ has image

$$s'\big((s \cdot -) \otimes f\big) = (ss' \cdot -) \otimes f.$$

To show functoriality in M, we want to show that for every $g \colon M \to M'$, the diagram

$$\begin{array}{ccc} S \otimes_R \mathrm{Hom}_R(M, N) & \xrightarrow{\theta} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\ {\scriptstyle \mathrm{id}_S \otimes (- \circ g)} \uparrow & & \uparrow {\scriptstyle - \circ (\mathrm{id}_S \otimes g)} \\ S \otimes_R \mathrm{Hom}_R(M', N) & \xrightarrow{\theta'} & \mathrm{Hom}_S(S \otimes_R M', S \otimes_R N) \end{array}$$

commutes. By S-linearity, it suffices to check this on pure tensors $s \otimes f$, where $f \colon M \to N$. Going up and right gives $s \otimes (f \circ g)$ then $(s \cdot -) \otimes (f \circ g)$. Going right and up gives $((s \cdot -) \otimes f)$ then

$$\big((s \cdot -) \otimes f\big) \circ (\mathrm{id}_S \otimes g) = (s \cdot -) \otimes (f \circ g),$$

which are equal. To show functoriality in N, we want to show that for every $h \colon N' \to N$, the diagram

$$\begin{array}{ccc} S \otimes_R \mathrm{Hom}_R(M, N) & \xrightarrow{\theta} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\ {\scriptstyle \mathrm{id}_S \otimes (h \circ -)} \downarrow & & \downarrow {\scriptstyle (\mathrm{id}_S \otimes h) \circ -} \\ S \otimes_R \mathrm{Hom}_R(M, N') & \xrightarrow{\theta'} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N') \end{array}$$

commutes. Again by S-linearity, it suffices to check this on pure tensors $s \otimes f$, where $f\colon M \to N$. Going down and right gives $(s \cdot -) \otimes (h \circ f)$. Going right and down gives

$$(\mathrm{id}_S \otimes h) \circ \big((s \cdot -) \otimes f\big) = (s \cdot -) \otimes (h \circ f).$$

Now suppose $R \to S$ is flat. Let

$$R^{\oplus J} \longrightarrow R^{\oplus I} \longrightarrow M \longrightarrow 0$$

be a presentation where I is finite (resp. both I and J are finite). By the functoriality in M described above, we have the commutative diagram

$$\begin{array}{ccc}
S \otimes_R \mathrm{Hom}_R(R^{\oplus J}, N) & \xrightarrow{\theta_{R^{\oplus J}}} & \mathrm{Hom}_S(S \otimes_R R^{\oplus J}, S \otimes_R N) \\
\uparrow & & \uparrow \\
S \otimes_R \mathrm{Hom}_R(R^{\oplus I}, N) & \xrightarrow{\theta_{R^{\oplus I}}} & \mathrm{Hom}_S(S \otimes_R R^{\oplus I}, S \otimes_R N) \\
\uparrow & & \uparrow \\
S \otimes_R \mathrm{Hom}_R(M, N) & \xrightarrow{\theta_M} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\
\uparrow & & \uparrow \\
0 & & 0
\end{array}$$

with exact columns. Now since I is finite (resp. I and J are finite), the map $\theta_{R^{\oplus I}}$ is an isomorphism (resp. $\theta_{R^{\oplus I}}$ and $\theta_{R^{\oplus J}}$ are isomorphisms): we have an isomorphism of functors

$$S \otimes_R \mathrm{Hom}_R(R^{\oplus I}, -) \xrightarrow{\sim} \mathrm{Hom}_S(S \otimes_R R^{\oplus I}, S \otimes_R -)$$

since they both represent the functor sending an R-module N to the set of $|I|$-tuples of elements in $S \otimes_R N$. By chasing around elements of the form $s \otimes f \in S \otimes_R \mathrm{Hom}_R(M, N)$, we see that θ_M is injective. If J is also finite, then θ_M is an isomorphism since isomorphic maps have isomorphic kernels. □

This is false without finite generation:

[Hoc17, p. 97] Example 7.7.5. Let M be the free $\mathbf{Z}$-module on countably many generators b_i and let $N = \mathbf{Z}$. An element $\mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z})$ corresponds to sequences of integers n_i that are the images of the b_i. Now let $S = \mathbf{Z}[1/p]$. The elements of

$$S \otimes_R \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Z})$$

correspond to sequences of fractions in $\mathbf{Z}[1/p]$ with bounded denominators, whereas sequences corresponding to elements of

$$\mathrm{Hom}_S(S \otimes_R M, S)$$

can have unbounded denominators, for example the sequence defined by $b_i/1 \mapsto 1/p^i$.

7.8. Projective modules

Proposition 7.7.1 suggests the following modules are special:

[AK21, (5.20)] [Hoc17, p. 88] Definition 7.8.1. Let R be a ring. We say that a module P over R is *projective* if $\mathrm{Hom}_R(P, -)$ is exact, and that a module I over R is *injective* if $\mathrm{Hom}_R(-, I)$ is exact.

We will focus more projective modules.

LEMMA 7.8.2. *An R-module is projective if and only if it is a direct summand of a free module.* [AK21, (5.22)] [Hoc17, p. 90]

Proof. $\Rightarrow$. Let $\beta\colon F \twoheadrightarrow P$ be a surjection from a free module. Applying $\mathrm{Hom}_R(P,-)$, we obtain a surjection

$$\mathrm{Hom}_R(P,F) \twoheadrightarrow \mathrm{Hom}_R(P,P),$$

and hence there exists a map $s\colon P \to F$ such that $\beta \circ s = \mathrm{id}_P$. This is exactly the condition that P is a direct summand of F by Problem 1 on Homework 4.

$\Leftarrow$. Let $P \subseteq F$ be the map realizing P as a direct summand of a free module. It suffices to show that for every surjection $M \twoheadrightarrow N$, the map $\mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,N)$ is surjective. But this fits into the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(P,M) & \longrightarrow & \mathrm{Hom}_R(P,N) \\ \uparrow\!\!\uparrow & & \uparrow\!\!\uparrow \\ \mathrm{Hom}_R(F,M) & \longrightarrow & \mathrm{Hom}_R(F,N) \end{array}$$

where the vertical arrows are surjective by the fact that they have a section. If the bottom arrow is surjective, then the top arrow is also surjective. □

EXAMPLE 7.8.3. Not all projective modules are free: If $R = R_1 \times R_2$, each factor R_i is a projective module, but is not free. [Hoc17, p. 88]

7.9. A projective module that is not free

We give the following more interesting example of a projective module that is not free, for which the important input is topological.

EXAMPLE 7.9.1 (Kaplansky; see [Swa62, Example 1]). Let [Hoc17, pp. 88–89]

$$A = \frac{\mathbf{R}[X,Y,Z]}{(X^2+Y^2+Z^2-1)}.$$

We denote the images of X, Y, and Z by x, y, and z, respectively. The elements of A can be considered as $\mathbf{R}$-valued polynomial functions on the unit 2-sphere centered at the origin on $\mathbf{R}^3$, and hence give continuous functions on the 2-sphere S^2.

Consider the A-linear map

$$f\colon A^{\oplus 3} \xrightarrow{\begin{pmatrix} x & y & z \end{pmatrix}} A.$$

We have a map

$$g\colon A \xrightarrow{\begin{pmatrix} x \\ y \\ z \end{pmatrix}} A^{\oplus 3}$$

and we set $u = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$. The composition $f \circ g$ is the matrix whose single entry is $x^2+y^2+z^2 = 1$, and so $f \circ g$ is the identity on A. We therefore see that

$$Q = \ker(f) \subseteq A^{\oplus 3}$$

is a projective A-module.

We claim that Q is not free. We proceed by contradiction. Base changing to the fraction field $K = \mathrm{Frac}(A)$, we see that $K^{\oplus 3} \cong K \oplus (K \otimes_A Q)$, and hence Q is a free module generated by two elements. It therefore suffices to show that $Q \cong A^{\oplus 2}$ yields a contradiction.

Suppose that Q has a free basis consisting of column vectors v and w in $A^{\oplus 3}$. Consider the 3×3 matrix

$$M = \begin{pmatrix} | & | & | \\ u & v & w \\ | & | & | \end{pmatrix}.$$

Since u, v, w span $A^{\oplus 3}$, there cannot be any linear relation on them, since their images in $K^{\oplus 3}$ form a basis as a K-vector, and hence cannot have any linear relations over K, either. Thus, u, v, w are a basis for $A^{\oplus 3}$, and the matrix M gives an automorphism of $A^{\oplus 3}$ with inverse matrix N. Computing determinants, we have

$$\det(M)\det(N) = 1,$$

and hence $\det(M)$ is a unit $\alpha \in A$. We can then multiply the second column of M by α^{-1}:

$$\begin{pmatrix} | & | & | \\ u & \alpha^{-1}v & w \\ | & | & | \end{pmatrix}.$$

Thus, we see that u is the first column of a 3×3 matrix over A with determinant 1.

We claim no such 3×3 matrix can exist, even with entries being continuous functions on S^2. If the third column is $w = \left(\begin{smallmatrix} f \\ g \\ h \end{smallmatrix}\right)$, then the vector-valued function

$$V = \begin{pmatrix} f \\ g \\ h \end{pmatrix} - (xf + yg + zh) \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

is a continuous vector-valued function on S^2 that does not vanish on S^2 since for every point $(a, b, c) \in S^2$, the two vectors u and w are linearly independent. Moreover, the value of V is orthogonal to the unit vector (a, b, c) for every $(a, b, c) \in S^2$, since the dot product vanishes. This means V is a everywhere non-vanishing continuous tangent vector field on S^2. This contradicts the hedgehog theorem!

7.10. Projective modules over local rings

10/21

Next, we want to show the following:

[AK21, (10.20)]
[Hoc17, p. 103]

THEOREM 7.10.1. *Let M be a module over a ring R. Consider the following conditions:*

(*i*) *M is free;*
(*ii*) *M is projective;*
(*iii*) *M is flat.*

Then, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Moreover, if R is local and M is finitely presented, then all three conditions are equivalent.

To prove this in the non-Noetherian case, we will use the following:

[Stacks, Tag 0519]
[AK21, (5.18)]

LEMMA 7.10.2. *Let R be a ring and let M be a finitely presented R-module. For every surjection $M' \twoheadrightarrow M$ where M' is finitely generated, the kernel N is finitely generated.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} & & R^{\oplus m'} & \longrightarrow & R^{\oplus m} & \longrightarrow & M & \longrightarrow & 0 \\ & & \vdots & & \downarrow & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

where we send the free generators of $R^{\oplus m}$ to elements on M' that make the right square commute. The dashed arrow exists by the universal property of kernels. By the snake lemma, we have an isomorphism

$$\operatorname{coker}(R^{\oplus m'} \to N) \xrightarrow{\sim} \operatorname{coker}(R^{\oplus m} \to M').$$

The cokernel of $R^{\oplus m} \to M'$ is finitely generated, and hence N is finitely generated by combining the sets of generators for $\operatorname{im}(R^{\oplus m'} \to N)$ and $\operatorname{coker}(R^{\oplus m'} \to N)$. □

We can now show Theorem 7.10.1.

Proof of Theorem 7.10.1. We saw already that (*i*) ⇒ (*ii*). To see that projective modules are flat, we need to show that for every injection $N' \hookrightarrow N$, the induced map $M \otimes_R N' \to M \otimes_R N$ is injective. Let $M \subseteq F$ be the map realizing M as a direct summand of a free module. Then, we have the commutative diagram

$$\begin{array}{ccc} M \otimes_R N' & \longrightarrow & M \otimes_R N \\ \downarrow & & \downarrow \\ F \otimes_R N' & \longrightarrow & F \otimes_R N \end{array}$$

where the vertical arrows are injective since they have a retraction. Since free modules are flat, the bottom arrow is injective, and hence the top arrow is injective as well.

It remains to consider the case when R is local and M is finitely presented. We will in fact show that the three conditions are equivalent to the following:

(*iv*) The map $\mathfrak{m} \otimes_R M \to M$ sending $r \otimes u$ to u is injective, where $\mathfrak{m} \subseteq R$ is the maximal ideal of R.

Since (*iii*) ⇒ (*iv*) by applying $M \otimes_R -$ to the injection $\mathfrak{m} \subseteq R$, it suffices to show that (*iv*) ⇒ (*i*).

Choose a minimal set of generators $u_1, u_2, \ldots, u_n$ for M and map $R^{\oplus n}$ onto M such that the ith generator maps to u_i. We then have a short exact sequence

$$0 \longrightarrow N \longrightarrow R^{\oplus n} \longrightarrow M \longrightarrow 0.$$

We also have the short exact sequence

$$0 \longrightarrow \mathfrak{m} \longrightarrow R \longrightarrow k \longrightarrow 0,$$

where k is the residue field of R. We now tensor these two short exact sequences together to obtain the commutative diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & \mathfrak{m}\otimes_R N & \longrightarrow & \mathfrak{m}\otimes_R R^{\oplus n} & \longrightarrow & \mathfrak{m}\otimes_R M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \\
0 & \longrightarrow & N & \longrightarrow & R^{\oplus n} & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & k\otimes_R N & \xrightarrow{f} & k\otimes_R R^{\oplus n} & \xrightarrow{g} & k\otimes_R M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The rows are obtained by applying $\mathfrak{m}\otimes_R -$, $R\otimes_R -$, and $k\otimes_R -$, respectively, and the columns are obtained by applying $-\otimes_R N$, $-\otimes_R R^{\oplus n}$, and $-\otimes_R M$, respectively. The hypothesis is used to show that α is injective. By minimality of the set of generators $u_1, u_2, \ldots, u_n$, we see that g is an isomorphism $k^{\oplus n} \to k^{\oplus n}$.

We claim it suffices to show that $k\otimes_R N = 0$. Note that N is finitely generated by Lemma 7.10.2. This would mean that $\mathfrak{m}\otimes_R N \to N$ is surjective, i.e., that $\mathfrak{m}N = N$, and hence NAK would show that $N = 0$. This would show that $R^{\oplus n} \to M$ is an isomorphism.

Let $u \in k\otimes_R N$; we want to show it is zero. By exactness in the bottom row, since g is an isomorphism, $f(u) = 0$. By exactness in the left column, there exists an element $v \in N$ that maps to u. The image of v in $R^{\oplus n}$ still maps to zero when mapped to $k\otimes_R R^{\oplus n}$, and hence v is the image of an element $w \in \mathfrak{m}\otimes_R R^{\oplus n}$. Suppose that w maps to an element $x \in \mathfrak{m}\otimes_R M$. Then $\alpha(x) = 0$ by the commutativity of the diagram, and hence by the injectivity of α, we see that $x = 0$. This shows that w is the image of an element $y \in \mathfrak{m}\otimes_R N$. Since w maps to v, y maps to v in N by injectivity of $N \to R^{\oplus n}$. This shows that v maps to zero in $k\otimes_R N$. But v maps to u, and hence $u = 0$. □

Corollary 7.10.3. *Let R be a ring, and let M be a finitely presented R-module. The following are equivalent:*

(*i*) *M is projective.*
(*ii*) *M is flat.*
(*iii*) *M is locally free, i.e., for every prime ideal $P \subseteq R$, the localization M_P is free over R_P.*

Proof. We know that projective modules are flat by Theorem 7.10.1. Now if M is flat, then M_P is flat, since for every inclusion $N' \subseteq N$, the map $M_P \otimes_R N' \to M_P \otimes_R N$ can be identified with $R_P \otimes_R M \otimes_R N' \to R_P \otimes_R M \otimes_R N$, and both M and R_P are flat over R. Thus, if M is flat, then M_P is flat for every prime ideal $P \subseteq R$.

Finally, we claim that if M is locally free, then M is projective. We want to show that for every surjection $N \twoheadrightarrow N'$, the map $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N')$ is surjective. By the fact that surjectivity is local and flat base change, this holds if and only if

$$\mathrm{Hom}_{R_P}(M_P, N_P) \longrightarrow \mathrm{Hom}_{R_P}(M_P, N'_P)$$

is surjective for every P. But this holds because M_P is free, whence projective by Lemma 7.8.2. □

7.11. Tensor products of algebras

The last thing I want to describe before moving to a different topic is how to take tensor products of algebras.

Definition 7.11.1. Let A be a ring, and let R and S be A-algebras. There is then an A-bilinear map [AK21, (8.20)] [Hoc17, p. 90] [AM69, pp. 30–31]

$$\begin{aligned} \mu\colon (R \otimes_A S) \times (R \otimes_A S) &\longrightarrow R \otimes_A S \\ (r \otimes s, r' \otimes s') &\longmapsto (rr') \otimes (ss') \end{aligned}$$

Using this A-bilinear map, one can define a ring structure on $R \otimes_A S$, which is in fact an A-algebra as well. This A-algebra comes equipped with maps

$$\begin{aligned} \iota_1\colon R &\longrightarrow R \otimes_A S & \qquad \iota_2\colon S &\longrightarrow R \otimes_A S \\ r &\longmapsto r \otimes 1 & \qquad s &\longmapsto 1 \otimes s \end{aligned}$$

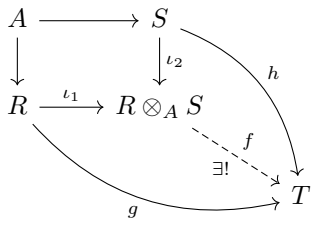
as A-algebras making the diagram

$$\begin{array}{ccc} A & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle \iota_2} \\ R & \xrightarrow{\iota_1} & R \otimes_A S \end{array}$$

commute. Note that [AM69, p. 31] has the wrong formula for the map $A \to R \otimes_A S$!

The tensor product has a universal property. This makes $R \otimes_A S$ the cofiber product of R and S over A in the category of commutative rings. We can also say that $R \otimes_A S$ is the coproduct in the category of R and S A-algebras.

Theorem 7.11.2. *For every A-algebra T making the outer diagram* [AK21, (8.20)] [Hoc17, pp. 90–91]



commute, there exists a unique dashed arrow making the entire diagram commute.

In terms of representable functors, this says that $R \otimes_A S$ represents the functor sending an A-algebra T to the set on the right below:

$$\begin{aligned} \mathrm{Hom}_{\mathsf{Alg}_A}(R \otimes_A S, T) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{Alg}_A}(R, T) \times \mathrm{Hom}_{\mathsf{Alg}_A}(S, T) \\ f &\longmapsto (f \circ \iota_1, f \circ \iota_2). \end{aligned}$$

Proof. Given such a diagram, we define an A-bilinear map

$$\begin{aligned} R \times S &\longrightarrow T \\ (r, s) &\longmapsto g(r) \cdot h(s) \end{aligned}$$

By the universal property of the tensor product, this defines a map of A-modules making the entire diagram commute. The fact that this is in fact a map of A-algebras follows by the formula defining the map. □

Example 7.11.3.

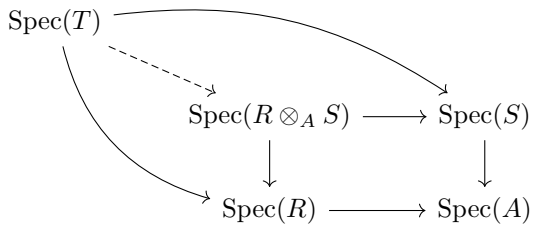
[Hoc17, p. 91]

(1) If A is a ring, the A-algebra $A[x] \otimes_A A[x]$ is *not* $A[x]$, but in fact is isomorphic to $A[x, y]$. In general, if R is an A-algebra, then $R \otimes_A A[x] \simeq R[x]$.

[AK21, (8.14)(2)] [AM69, Exer. 2.1]

(2) If $m, n \in \mathbf{Z}$ are coprime, then $(\mathbf{Z}/(m)) \otimes_{\mathbf{Z}} (\mathbf{Z}/(n)) = 0$.

Theorem 7.11.2 gives a geometric description of tensor products of rings. Applying Spec to the diagram in Theorem 7.11.2, we get the diagram



This gives $\operatorname{Spec}(R \otimes_A S)$ the structure of the *fiber product* in a certain category. One reason this terminology makes sense is that if we take $R = \kappa(P)$ for a prime ideal $P \subseteq A$ and $S = A[x]$, then $\operatorname{Spec}(\kappa(P) \otimes_A A[x]) \simeq \operatorname{Spec}(\kappa(P)[x])$ is the fiber of $\operatorname{Spec}(A[x]) \to \operatorname{Spec}(A)$ as topological spaces.

On the other hand, $\operatorname{Spec}(R \otimes_A S)$ is not always the fiber product as sets.

Example 7.11.4. Consider

$$\begin{array}{ccc} \operatorname{Spec}\big(k[x,y]\big) & \longrightarrow & \operatorname{Spec}\big(k[y]\big) \\ \downarrow & & \downarrow \\ \operatorname{Spec}\big(k[x]\big) & \longrightarrow & \operatorname{Spec}(k) \end{array}$$

for a field k. Then, $\operatorname{Spec}(k[x, y])$ has a point corresponding to the diagonal $(x - y)$ that is not in the product set $\operatorname{Spec}(k[x]) \times \operatorname{Spec}(k[y])$.

A question we had last time was the following: Given a ring map $R \to S$, when is $M \otimes_R N \twoheadrightarrow M \otimes_S N$ an isomorphism?

[Hoc17, pp. 91–92]

Example 7.11.5. We saw that $A[x] \otimes_A A[x] \twoheadrightarrow A[x] \otimes_{A[x]} A[x]$ is not an isomorphism. However, there are two cases when it is an isomorphism: when $R \to S$ is a quotient map of rings, or when $S = W^{-1}R$ for a multiplicative set. In the first case, the point is that any element of S is the image of an element in R that can be passed through the $\otimes$ symbol. In the second case, the point is that if we want to move r/w across the tensor symbol, then

$$\left(\frac{r}{w}\, u\right) \otimes v = \left(\frac{r}{w}\, u\right) \otimes \left(w\, \frac{1}{w}\, v\right) = ru \otimes \left(\frac{1}{w}\, v\right) = u \otimes \left(\frac{r}{w}\, v\right).$$

7.12. Examples

10/23

Before we give some more examples, we prove the following criterion for flatness:

[AK21, (9.24)]
[Liu02, Thm. 1.2.4]

LEMMA 7.12.1 (Ideal criterion for flatness). *A module M over a ring R is flat if and only if, for every ideal $I \subseteq R$, the inclusion $I \subseteq R$ induces an injection $I \otimes M \hookrightarrow M$, or equivalently, an isomorphism $I \otimes M \xrightarrow{\sim} IM$.*

Proof. The two latter conditions are equivalent since the $I \otimes M \hookrightarrow R \otimes M \simeq M$ is given by $i \otimes m \mapsto im$. The direction $\Rightarrow$ follows from the definition of flatness, and hence it suffices to show the converse.

Consider an inclusion $N' \subseteq N$. We first claim that if N is free of finite rank r, then $N' \otimes_R M \to N \otimes_R M$ is injective. The $r = 1$ case follows from hypothesis. The $r > 1$ follows by induction as follows: we can write $N \simeq N_1 \oplus N_2$ for free modules N_1 and N_2 of strictly smaller rank. Writing $N_1' = N_1 \cap N'$ and $N_2' = N_2 \cap N'$, we have the commutative diagram

$$\begin{array}{ccccccccc} & & N_1' \otimes_R M & \longrightarrow & N' \otimes_R M & \longrightarrow & N_2' \otimes_R M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 \otimes_R M & \longrightarrow & N \otimes_R M & \longrightarrow & N_2 \otimes_r M & \longrightarrow & 0 \end{array}$$

The left and right vertical arrows are injective by induction, and the rows are exact by right exactness of tensor products and by the fact that $N_1 \to N$ has a retraction, respectively. The snake lemma then implies that the middle vertical arrow is also injective.

Now we claim that if N is free of arbitrary rank, then $N' \otimes_R M \to N \otimes_R M$ is injective. Let $N_0 \subseteq N$ be a free direct summand. Then, the map $(N' \cap N_0) \otimes_R M \to N_0 \otimes_R M$ is injective. Thus, so is the map $(N' \cap N_0) \otimes_R M \to N \otimes_R M$, since the map $N_0 \to N$ has a retraction. Because for every $x \in N' \otimes_R M$ there exists an N_0 such that x is contained in the image of $(N' \cap N_0) \otimes M \to N' \otimes M$, we see that $N' \otimes M \to N \otimes M$ is injective.

Now let N be an arbitrary R-module. Then, there exists a free R-module L and a surjective map $p\colon L \to N$. Let $L' = p^{-1}(N')$. We then have the commutative diagram

$$\begin{array}{ccccccc} \ker(p) & \longrightarrow & L' & \longrightarrow & N' & \longrightarrow & 0 \\ \| & & \downarrow & & \downarrow & & \\ \ker(p) & \longrightarrow & L & \xrightarrow{p} & N & \longrightarrow & 0 \end{array}$$

with exact rows, giving the commutative diagram

$$\begin{array}{ccccccc} \ker(p) \otimes_R M & \longrightarrow & L' \otimes_R M & \longrightarrow & N' \otimes_R M & \longrightarrow & 0 \\ \| & & \downarrow & & \downarrow & & \\ \ker(p) \otimes_R M & \longrightarrow & L \otimes_R M & \xrightarrow{p} & N \otimes_R M & \longrightarrow & 0 \end{array}$$

Since the middle vertical arrow is injective, this shows the injectivity of $N' \otimes_R M \to N \otimes_R M$. □

COROLLARY 7.12.2. *Let R be a PID. An R-module M is flat if and only if it is torsion-free.* [AK21, (9.26)] [Liu02, Cor. 1.2.5]

Proof. The direction $\Rightarrow$ follows from definition of flatness: the multiplication map $R \xrightarrow{x\cdot} R$ is injective, and must stay injective after tensoring by M.

For $\Leftarrow$, we note that if M is finitely generated, this follows from the classification of finitely generated modules over a PID. If M is not finitely generated, we use the

ideal criterion. Let $I = (r) \subseteq R$ be an ideal. Then, the map $R \to I$ induced by multiplication by r is an isomorphism. The composition

$$R \otimes_R M \xrightarrow[\sim]{(r\cdot -)\otimes \mathrm{id}_M} I \otimes_R M \longrightarrow M$$

is injective since it is the multiplication by r map on M. Thus, $I \otimes_R M \to M$ is also injective, and hence M is flat. □

Example 7.12.3. We give some examples of tensor products in action. Both are flat by Corollary 7.12.2.

[Har77, Ex. II.3.3.1] (1) Consider the ring map

$$k[t] \longrightarrow \frac{k[x,y,t]}{(ty - x^2)}.$$

Taking spectra, we can think of the spectrum of the codomain as an algebraic family of parabolas $\{ty - x^2 = 0\} \subseteq k^2$ parametrized by t. The fiber over $t \neq 0$ is an honest parabola, but over $t = 0$ we get a non-reduced ring $k[x,y]/(x^2)$, the "double line" $\{x^2 = 0\}$.

[Har77, Ex. II.3.3.2] (2) Consider the ring map

$$k[t] \longrightarrow \frac{k[x,y,t]}{(xy - t)}.$$

This corresponds to a family of hyperbolas parametrized by t. When $t = 0$, you get the reduced ring $k[x,y]/(xy)$ that is not a domain.

[Har77, Ex. III.9.8.4] Example 7.12.4. Consider the family

$$\begin{cases} x = t^2 - 1 \\ y = t^3 - t \\ z = at \end{cases}$$

of parametric curves in k^3 parametrized by $a \in k$. This is a version of the twisted cubic we saw before. We want to turn this into a *flat* family. To do so, we eliminate t from the parametric equations, and make sure that a is not a zerodivisor in $k[a,x,y,z]/I$. This yields the flat map

$$k[a] \longrightarrow \frac{k[x,y,z,a]}{(a^2(x+1) - z^2, ax(x+1) - yz, xz - ay, y^2 - x^2(x+1))}$$

corresponding to a family of twisted cubics in k^3 parametrized by a when $a \neq 0$. When $a = 0$, you get the ring

$$\frac{k[x,y,z]}{(z^2, yz, xz, y^2 - x^2(x+1))},$$

which is non-reduced.

We have the following "permanence" properties for flatness.

[Hoc17, p. 98] Proposition 7.12.5. *Let $R \to S \to T$ be ring maps. If S is flat over R and T is flat over S, then T is flat over R.*

Proof. This holds since $- \otimes_R T \cong - \otimes_R S \otimes_S T$ as functors on Mod_R. □

[Hoc17, p. 98] Proposition 7.12.6. *If M is flat (resp. free, projective) over R, then $S \otimes_R M$ is flat (resp. free, projective) over S.*

Proof. This holds since $- \otimes_S S \otimes_R M \cong - \otimes_R M$ as functors on Mod_S. □

LEMMA 7.12.7. *If M and N are R-modules, $W \subseteq R$ is a multiplicative set, and $S = W^{-1}R$, then the natural R-module map* [Hoc17, p. 98]

$$M \otimes_R N \longrightarrow W^{-1}M \otimes_S W^{-1}N$$

induces an S-module isomorphism

$$W^{-1}(M \otimes_R N) \xrightarrow{\sim} W^{-1}M \otimes_S W^{-1}N.$$

Proof. Note the map comes from the universal properties of tensor products and of localization. The map is an isomorphism since we have natural isomorphisms

$$\begin{aligned} W^{-1}(M \otimes_R N) &\cong S \otimes_R (M \otimes_R N) \\ &\cong S \otimes_R S \otimes_R (M \otimes_R N) \\ &\cong (S \otimes_R M) \otimes_R (S \otimes_R N) \\ &\cong W^{-1}M \otimes_R W^{-1}N \\ &\cong W^{-1}M \otimes_S W^{-1}N \end{aligned}$$

where the second isomorphism holds since $S = W^{-1}R$. □

PROPOSITION 7.12.8. *M is flat over R if and only if M_P is flat over R_P for all prime (resp. maximal) ideals P.* [Hoc17, p. 98]

Proof. Combine Theorem 7.14.1(*d*) with Lemma 7.12.7. □

7.13. Colon ideals

The next topic will be the existence of primary decompositions. To work with primary decompositions, we will need colon ideals. These ideals will be used to extract primary components of an ideal given a primary decomposition.

DEFINITION 7.13.1. Let $I \subseteq R$ be an ideal in a ring R, and let S be an arbitrary subset of R. The *colon ideal* or *ideal quotient* of I and S is [Hoc17, p. 77] [AM69, p. 8]

$$(I :_R S) \coloneqq \{r \in R \mid \text{for all } s \in S, \text{ we have } rs \in I\}.$$

If J is the ideal generated by S, then $(I :_R J) = (I :_R S)$.

REMARK 7.13.2. The reason why it is called an ideal quotient is that $(I :_R J)J \subseteq I$. For example, $(\langle 6\rangle :_{\mathbf{Z}} 2) = \langle 3\rangle$. This suggests that colon ideals can be used to extract primary components from an ideal. [AM69, p. 8]

PROPOSITION 7.13.3. *Let $R \to S$ be a flat ring map, and let I and J be ideals of R, where J is finitely generated. Then, $(I :_R J)S = (IS :_R JS)$. In particular, this holds when S is a localization of R.* [Hoc17, p. 94] [AM69, p. 42]

In the proof below, we will identify $I \otimes_R S$ with its image IS in S. This is allowed since the surjection $I \otimes_R S \twoheadrightarrow IS$ is in fact an injection by flatness.

Proof. If $J = (f)$ is a principal ideal, then we consider the short exact sequence

$$0 \longrightarrow \frac{(I :_R f)}{I} \longrightarrow \frac{R}{I} \xrightarrow{f\cdot} \frac{R}{I}.$$

Extending scalars to S, we then have

$$0 \longrightarrow \frac{(I :_R f)S}{IS} \longrightarrow \frac{S}{IS} \xrightarrow{f\cdot} \frac{S}{IS}.$$

The kernel of multiplication by f on S/IS is $(IS :_R f)/IS$, and hence $(I :_R f)S/IS = (IS :_S f)/IS$. This shows $(I :_R f)S = (IS :_S f)$ by Proposition 1.3.12.

Now suppose that $J = (f_1, f_2, \ldots, f_h)$, then we have

$$(I :_R J) = \bigcap_{t=1}^{h} (I :_R f_t),$$

and since flat base change commutes with finite intersections (Lemma 7.13.4), we have

$$(I :_R J)S = (I :_R J) \otimes_R S = \left(\bigcap_{t=1}^{h} (I :_R f_t) \right) \otimes_R S$$

By the case for principal ideals proved above, this is equal to

$$\bigcap_{t=1}^{h} \big((I :_R f_t)S\big) = \bigcap_{t=1}^{h} (IS :_S f_t) = (IS :_S JS). \qquad \square$$

[Hoc17, p. 92] LEMMA 7.13.4. *Flat base change commutes with finite intersections.*

Proof. Consider the flat base change of $0 \to N_1 \cap N_2 \to N_1 \oplus N_2 \to M$, where $N_1, N_2 \subseteq M$ and the second map is $(u, v) \mapsto u - v$. $\square$

7.14. More local properties

A while ago, we discussed what properties of rings, modules, and maps can be detected locally. We can now add to our list. Note that we only stated and proved (f) and (g) in class.

[Hoc17, p. 95] THEOREM 7.14.1. *Let R be a ring, let $f\colon M \to M'$ be a map of R-modules, let $u \in M$, and let N, N_1, and N_2 be submodules of M. Below, "for all P" means "for all prime ideals P" or "for all maximal ideals P."*

- (a) *The formation of kernels, cokernels, and images commute with localization.*
- (b) *$u/1 \in M_P$ is nonzero if and only if $P \supseteq \operatorname{Ann}_R(u)$. The element $u = 0$ in M if and only if $u/1 = 0$ in M_P for all P.*
- (c) *$M = 0$ if and only if $M_P = 0$ for all P.*
- (d) *$f\colon M \to M'$ is injective (resp. surjective, bijective) if and only if f_P is injective (resp. surjective, bijective) for all primes P.*
- (e) *$u \in M$ is in N if and only if $u/1 \in M_P$ is in N_P for all primes P.*
- (f) *$N_1 \subseteq N_2$ (resp. $N_1 = N_2$) if and only if $(N_1)_P \subseteq (N_2)_P$ for all primes P.*
- (g) *$0 \to M' \to M \to M'' \to 0$ is exact if and only if $0 \to M'_P \to M_P \to M''_P \to 0$ is exact for all primes P, and $M' \to M \to M''$ is exact if and only if $M'_P \to M_P \to M''_P$ is exact for all P.*

Proof. We saw (c) in Proposition 3.5.1. We saw (d) in Corollary 3.5.3.

We prove all the statements below. (a) holds since the formation of kernels, cokernels, and images commute with flat base change.

For (b) and (c), set $I = \operatorname{Ann}_R(u)$. Then, the map

$$\begin{aligned} R &\longrightarrow R \cdot u \\ r &\longmapsto ru \end{aligned}$$

is surjective and has kernel I. Thus, $Ru \cong R/I$. Next, $(R/I)_P \neq 0$ if and only if $I \cap (R - P) = \emptyset$ if and only if $P \supseteq I$. The second statement in (b) holds because if

$u \neq 0$, then I is proper and there exists a maximal ideal P containing I. (c) holds since if $u \neq 0$ in M, then $Ru \hookrightarrow M$, and this is preserved when we localize at $P \supseteq I$.

(d) follows from (a) and (c): f is injective (resp. surjective, bijective) if and only if $\ker(f) = 0$ (resp. $\operatorname{coker}(f) = 0$, $\ker(f) = \operatorname{coker}(f) = 0$) if and only if $\ker(f)_P = 0$ (resp. $\operatorname{coker}(f)_P = 0$, $\ker(f)_P = \operatorname{coker}(f)_P = 0$) for all P.

(e) follows by applying (b) to $\bar{u} \in M/N$.

For (f), we have $N_1 \subseteq N_2$ if and only if $N_1/(N_1 \cap N_2) = 0$. The result now follows by the fact that localization commutes with finite intersections together with (c). The second part follows by applying the first part to $N_1 \subseteq N_2$ and $N_2 \subseteq N_1$. Alternatively, one can say $N_1 = N_2$ if and only if $(N_1 + N_2)/(N_1 \cap N_2) = 0$.

For (g), it suffices to show the second statement. This statement follows from (a) and (f). □

Splitting is a local condition, but only for finitely presented modules.

PROPOSITION 7.14.2. *Let R be a ring and let $Q = M/N$ be a finitely presented module over R. Then, the short exact sequence* [Hoc17, p. 97]

$$0 \longrightarrow N \longrightarrow M \xrightarrow{f} Q \longrightarrow 0$$

splits if and only if

$$0 \longrightarrow N_P \longrightarrow M_P \xrightarrow{f_P} Q_P \longrightarrow 0$$

splits for every prime (resp. maximal) ideal P.

Proof. The short exact sequence splits if and only if

$$\operatorname{Hom}_R(Q, N) \longrightarrow \operatorname{Hom}_R(Q, Q)$$

is surjective. This holds if and only if

$$\operatorname{Hom}_R(Q, N)_P \longrightarrow \operatorname{Hom}_R(Q, Q)_P$$

is surjective for every P. By flat base change, this holds if and only if

$$\operatorname{Hom}_{R_P}(Q_P, N_P) \longrightarrow \operatorname{Hom}_{R_P}(Q_P, Q_P)$$

is surjective for every P. □

PROPOSITION 7.14.3. *Let R be a ring. Below, "for all P" means "for all prime ideals P" or "for all maximal ideals P."* [Hoc17, p. 98]

(a) *R is reduced if and only if R_P is reduced for all P.*
(b) *If R is a domain, then R is normal if and only if R_P is normal for all P.*
(c) *If R is Noetherian, or more generally, if R has only finitely many minimal primes, then R is a domain if and only if* $\operatorname{Spec}(R)$ *is connected and R_P is a domain for all P.*

Proof. (a) was shown in Proposition 3.5.2. (b) follows by applying Theorem 7.14.1(f) to the inclusion $R \to \bar{R}$.

It remains to show (c). We know that if R is a domain, then R_P is a domain for every P and $\operatorname{Spec}(R)$ is connected: $\operatorname{Spec}(R)$ is not connected if and only if R contains an idempotent e other than $0, 1$, and the equation $e(1-e) = 0$ implies $e = 0$ or $e = 1$. Now suppose that $\operatorname{Spec}(R)$ is connected and that R_P is a domain for all P. By (a), R is reduced. Now let $P_1, P_2, \ldots, P_k$ be the minimal primes of R. The union of closed set $V(P_t)$ is $\operatorname{Spec}(R)$, since every prime contains a minimal prime. Moreover, the $V(P_t)$ are mutually disjoint, for if Q contains both P_i and P_j, then

R_Q has at least two minimal primes, and hence is not a domain. Thus, the $V(P_t)$ are open as well as closed, and hence the assumption that $\mathrm{Spec}(R)$ is connected implies there is a unique minimal prime P. Since R is reduced, $P = \sqrt{(0)} = (0)$, and hence (0) is prime and R is a domain. $\square$

CHAPTER 8

Primary decomposition

8.1. Motivation

10/25

The original motivation for primary decomposition comes from number theory. Every integer n can be written as

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

by prime factorization. The question is then: how does this generalize to other number rings, or even to arbitrary rings? The trick is to replace prime numbers by prime ideals, and powers of prime numbers by what are called *primary ideals*. So we will discuss for a while what primary ideals are, and how to show that in Noetherian rings, every ideal can be written as an intersection of primary ideals. Flatness and localization will be used to study such decompositions.

This theory is due to Emanuel Lasker [Las1905] for polynomial rings finitely generated over a field and due to Emmy Noether [Noe1921] in arbitrary Noetherian rings.

8.2. Primary ideals

These ideals are the analogue of prime powers in $\mathbf{Z}$ or in PID's.

DEFINITION 8.2.1. An ideal $I \subseteq R$ is *primary* if $xy \in I$ implies $x \in I$ or $y \in \sqrt{I}$. [Rei95, p. 103] [Hoc17, p. 105]

REMARK 8.2.2. While the definition may look asymmetric, the point is that one has to check products of the form xy *and* products of the form yx. In other words, $I \subseteq R$ is primary if and only if $xy \in I$ implies $x \in I$, $y \in I$, or $x, y \in \sqrt{I}$.

LEMMA 8.2.3. *If an ideal $I \subseteq R$ is primary, then $\sqrt{I}$ is prime.* [Rei95, p. 104] [Hoc17, p. 105] [AM69, Prop. 4.1]

Proof. If $xy \in \sqrt{I}$, then $x^n y^n \in I$ for some n, and hence either $x^n \in I$ or $y^n \in \sqrt{I}$. But this implies $x \in \sqrt{I}$ or $y \in \sqrt{I}$. □

DEFINITION 8.2.4. Let $I \subseteq R$ be a primary ideal, and let $P = \sqrt{I}$. We then say that I is *primary* to the prime ideal P. [Rei95, p. 104] [Hoc17, p. 105] [AM69, p. 50]

EXAMPLE 8.2.5. The converse of the above is false: the ideal $I = (x^2, xy) \subseteq k[x, y]$ has radical (x), which is prime. But $xy \in I$, whereas $x \notin I$ and $y \notin \sqrt{I}$. [Rei95, p. 104] [Hoc17, p. 105]

The converse does hold, however, when $\sqrt{I}$ is maximal.

PROPOSITION 8.2.6. *Let R be a ring and let $I \subseteq R$ be an ideal with radical P.* [Hoc17, p. 105] [AM69, p. 50, Prop. 4.2]

(*i*) *If P is maximal, then I is primary to P.*

(*ii*) *Suppose P is prime. Then, I is P-primary if and only if $xy \in I$ and $y \in R - P$ implies $x \in I$. Moreover, the ideals primary to P are in bijective correspondence with the ideals primary to the maximal ideal PR_P of R_P.* [Rei95, p. 104] [AM69, Prop. 4.8]

(*iii*) *I is primary to P if and only if P/I is prime and the elements of $R - P$ are not zerodivisors on R/I, that is, if and only if the nilpotent elements in R/I form a prime ideal (which will necessarily be equal to the unique minimal prime), and the elements that are not nilpotent in R/I are not zerodivisors.*

(*iv*) *If $J \subseteq I$ then I is primary to P if and only if I/J is primary to P/J in R/J.*

Proof. For (*i*), we proceed by contradiction. Suppose $xy \in I$ but that $y \notin \sqrt{I}$. Since $P = \sqrt{I}$ is maximal, we have $\sqrt{I} + (y) = R$. By the Scheinnullstellensatz (see Proposition 1.6.3), we have

$$\sqrt{I} + (y) = R \iff V\big(\sqrt{I} + (y)\big) = \emptyset \iff V\big(I + (y)\big) = \emptyset \iff I + (y) = R.$$

There therefore exist $i \in I$ and $r \in R$ such that $i + ry = 1$. Then, $x = x(i + ry) = xi + rxy \in I$, since both i and xy lie in I.

(*ii*) is a restatement of the definition of what it means to be primary assuming Lemma 8.2.3. The second statement follows from a slight generalization of the correspondence of ideals for the localization map $R \to R_P$ in Proposition 3.2.10 (see [AK21, (11.20)]).

(*iii*) is a restatement of (*iii*) since P is prime if and only if P/I is prime, and since the image of $y \in R - P$ in P/I is not a zerodivisor if and only if for all $x \in R$, $xy \in I$ implies $x \in I$.

(*iv*) follows from (*iii*): I is primary to P if and only if P/I is prime and the elements of $R - P$ are not zerodivisors on R/I if and only $(P/J)/(I/J)$ is prime and the elements of $R - P$ are not zerodivisors on $(R/J)/(I/J)$ if and only if I/J is primary to P/J. □

We now prove some facts about the behavior of primary ideals under operations on ideals.

[Hoc17, p. 106]
[Rei95, p. 106]
[AM69, Lem. 4.3]
[AM69, p. 50]

Proposition 8.2.7. *Let R be a ring and let P be a prime ideal.*

(*i*) *The intersection of finitely many P-primary ideals is P-primary.*

(*ii*) *If $R \to S$ is a ring map, and J is an ideal of S primary to a prime ideal Q lying over P in R, then the contraction I of J to R is primary to P.*

Proof. For (*i*), by induction it suffices to show that if I_1 and I_2 are P-primary, then so is $I_1 \cap I_2$. We first see that $\sqrt{I_1 \cap I_2} = P$ since $\subseteq$ holds automatically, and every element of P has a power in I_1 and a power in I_2, and the higher of these two powers will be in $I_1 \cap I_2$. Now suppose $xy \in I_1 \cap I_2$ and $x \notin I_1 \cap I_2$. Then, $x \notin I_t$ for $t = 1$ or $t = 2$. In either case, we have $y \in \sqrt{I_t} = P = \sqrt{I_1 \cap I_2}$.

For (*ii*), we have an injection $R/I \hookrightarrow S/J$, since I is the contraction of J to R. By Proposition 8.2.6(*iii*), it suffices to show that P/I is prime and the elements of $R - P$ are not zerodivisors on R/I. P/I is prime since it is the contraction of Q/J under the injection $R/I \hookrightarrow S/J$. This injection induces an injection $R/I - P/I \hookrightarrow S/J - Q/J$, and hence elements in $R - P$ are not zerodivisors on R/I by applying Proposition 8.2.6(*iii*) to J in S. □

8.3. Primary decompositions

[AK21, (18.13)]
[Rei95, p. 105]
[Hoc17, p. 106]
[AM69, p. 51]

Definition 8.3.1. A *primary decomposition* of an ideal I is a representation

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_r$$

of I as a finite intersection of primary ideals Q_i.

Given such a decomposition, if several of the ideals have the same radical, we may intersect them to give a decomposition with fewer ideals. If some proper subset of the primary ideals has the same intersection, we can work with that proper subset instead of the whole subset. Thus, if an ideal I has a primary decomposition, it has a primary decomposition such that

(1) $\sqrt{Q_i} \neq \sqrt{Q_j}$ if $Q_i \neq Q_j$, i.e., radicals of mutually distinct ideals are mutually distinct primes.
(2) For every j, we have $I \subsetneq \bigcap_{i \neq j} Q_i$, i.e., no term may be omitted without strictly increasing the intersection.

DEFINITION 8.3.2. A primary decomposition satisfying (1) and (2) is called a *irredundant* primary decomposition. [AK21, (18.13)] [Rei95, p. 105] [Hoc17, p. 106] [AM69, p. 52]

We will prove that every ideal in a Noetherian ring has an irredundant primary decomposition satisfying the following uniqueness properties:

- The number of ideals occurring is unique.
- The set of primes $\{\sqrt{Q_i}\}_i$ is unique.
- The set of primary ideals whose radicals are *minimal* in the set $\{\sqrt{Q_i}\}_i$ is unique.

DEFINITION 8.3.3. Let $I = Q_1 \cap Q_2 \cap \cdots \cap Q_r$ be a primary decomposition. The *minimal primes* of I are the primes minimal in the set $\{\sqrt{Q_i}\}_i$. The other primes are called *embedded primes*. [Rei95, p. 106] [Hoc17, p. 106] [AM69, p. 52]

We give an example that shows that primary decompositions are not completely unique, which also explains this terminology.

EXAMPLE 8.3.4. Let $I = (x^2, xy) \subseteq k[x, y]$, where k is a field. Then, by looking at monomials that appear in polynomials contained in each ideal, we have that [AK21, (18.14)] [Rei95, p. 106] [Hoc17, pp. 106–107] [AM69, p. 52]

$$(x^2, xy) = (x) \cap (x^2, y)$$

is an irredundant primary decomposition: (X) is prime, and $\sqrt{(x^2, y)} = (x, y)$ is maximal. They are minimal and embedded primes, respectively.

Now for every element $c \in k$, the elements $x, cx + y$ also generate R, and the elements x and $cx + y$ are algebraically independent. We have

$$(x^2, xy) = \big(x^2, x(cx + y)\big).$$

We therefore also have

$$(x^2, xy) = (x) \cap (x^2, x + cy).$$

One can show that each of the ideals on the right-hand side are distinct for distinct values of c (if $Q = (x^2, x+cy) = (x^2, x+c'y)$, then $(x+cy)-(x+c'y) = (c-c')y \in Q$, in which case $x = (x + cy) - cy \in Q$). We can also write

$$(x^2, xy) = (x) \cap (x^2, xy, y^2).$$

8.4. Existence of primary decompositions

For Noetherian rings, the fact that primary decompositions exist will follow from the existence of *irreducible* decompositions.

DEFINITION 8.4.1. Let $I \subsetneq R$ be a proper ideal in a ring R. We say that I is *irreducible* or *indecomposable* if it is not the intersection of two (equivalently finitely many) strictly larger ideals.

[Rei95, p. 108] [Hoc17, p. 107] [AM69, p. 82]

The following says that every proper ideal in a Noetherian ring is the intersection of finitely many irreducible ideals. We will then show that irreducible ideals are primary.

[Rei95, p. 108] [Hoc17, p. 107] [AM69, Lem. 7.11]

PROPOSITION 8.4.2. *Every proper ideal in a Noetherian ring is the intersection of a finite family of irreducible ideals (if the ideal is irreducible, the family has just one element).*

Proof. We prove this using a form of Noetherian induction. Let Σ be the set of ideals not expressible as the intersection of irreducibles. We claim that $\Sigma = \emptyset$. If not, then Σ contains a maximal element $I \in \Sigma$, which cannot be irreducible, so $I = J \cap K$ for J and K strictly containing I. The ideals J and K must be proper, for otherwise if $J = R$, then $K = I$, or vice versa. By maximality, J and K are not in Σ, and hence they are intersections of finitely many irreducibles. Thus, we can write I as the intersection of the sets of irreducibles whose intersections are J and K respectively. □

10/28

We can now prove that primary decompositions exist.

[AK21, (18.21)] [Rei95, p. 108] [Hoc17, p. 108] [AM69, Lem. 7.12, Thm. 7.13]

THEOREM 8.4.3. *Let R be a Noetherian ring and let I be an irreducible ideal of R. Then, I is primary. As a consequence, every proper ideal I in a Noetherian ring has an irredundant primary decomposition.*

Proof. Let $xy \in I$, and suppose that $x \notin I$. We want to show that $y \in \sqrt{I}$. Consider the sequence of ideals $(I :_R y^n)$. This sequence is non-decreasing, and by Noetherianity, this sequence stabilizes. Thus, there exists an integer $N > 0$ such that

$$\bigcup_{n \geq 0} (I :_R y^n) = (I :_R y^N).$$

We claim that $y^N \in I$. For sake of contradiction, suppose that $y^N \notin I$, in which case $I + (y^N) \supsetneq I$. We will show that

$$I = \big(I + (y^N)\big) \cap (I :_R y^N),$$

which will contradict the irreducibility of I. Suppose $u = i + ry^N$ is in this intersection, where $i \in I$ and $r \in R$. Since this element is also in $(I :_R y^N)$, we see that

$$(i + ry^N)y^N = iy^N + ry^{2N} \in I,$$

which implies that $ry^{2N} \in I$. Thus, $r \in (I :_R y^{2N}) = (I :_R y^N)$. Since $ry^N \in I$, we therefore see that $u = i + ry^N \in I$ as well, as required. □

8.5. Uniqueness of primary decompositions

We now state the uniqueness result for primary decompositions.

[AK21, (18.20), (18.25)] [Rei95, pp. 109–110] [Hoc17, pp. 108–109] [AM69, Thm. 4.5, Prop. 4.6, Thm. 4.10, Cor. 4.11, Prop. 7.17]

THEOREM 8.5.1. *Let R be a ring and suppose that an ideal $I \subseteq R$ has an irredundant primary decomposition*

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n.$$

We then have the following:

(*i*) *Each prime ideal $P_i = \sqrt{Q_i}$ is distinct.*
(*ii*) *The set of prime ideals $\{P_i\}$ is uniquely determined. More precisely, a prime P occurs if and only if $P = \sqrt{(I :_R r)}$ for some $r \in R$. Thus, the number of terms n in the decomposition is uniquely determined.*
(*iii*) *The minimal primes in $\{P_i\}$ give an irredundant primary decomposition of $\sqrt{I}$, and are the same as the minimal primes of I.*
(*iv*) *For each minimal prime P in $\{P_i\}$, the primary ideal Q corresponding to it is the contraction of IR_P to R, and so is uniquely determined.*

Before we prove this, we need the following lemma, which explains how colon ideals extract primary components.

LEMMA 8.5.2. *Let R be a ring.* [Hoc17, p. 109] [AM69, Lem. 4.4]

(*i*) *If $I_1, I_2, \dots, I_n$ are ideals in R, then*

$$\sqrt{I_1 \cap I_2 \cap \cdots \cap I_n} = \sqrt{I_1} \cap \sqrt{I_2} \cap \cdots \sqrt{I_n}.$$

(*ii*) *If $P_1, P_2, \dots, P_k$ are mutually incomparable prime ideals, then the P_i are the minimal primes of $P_1 \cap P_2 \cap \cdots \cap P_k$.*
(*iii*) *If Q is primary to P, then*

$$\sqrt{(Q :_R r)} = \begin{cases} R & \text{if } r \in Q; \\ P & \text{if } r \notin Q. \end{cases}$$

Moreover, if $r \notin P$, then $(Q :_R r) = Q$.

Proof. We already saw (*i*) for two ideals in Proposition 8.2.7. The inclusion $\subseteq$ is clear: intersections of radical ideals are radical. For the other direction, if an element x is in the right-hand side, then $x^{a_t} \in I_t$ for some $a_1, a_2, \dots, a_n$. Taking the maximum of the a_t gives a power x^a of x that lies in all of the I_t.

For (*ii*), it suffices to show that if $P \supseteq P_1 \cap P_2 \cap \cdots \cap P_k$, then $P \supseteq P_i$ for some i. If not, choose $r_i \in P_i - P$ for every i. Then, $\prod_j r_j \in P_i$ for every i, but does not lie in P, a contradiction.

For (*iii*), we first have

$$r \in Q \implies (Q :_R r) = R \implies \sqrt{(Q :_R r)} = R.$$

We now suppose $r \notin Q$. Since $Q \subseteq (Q :_R r)$, we have $P = \sqrt{Q} \subseteq \sqrt{(Q :_R r)}$. To show the converse, it suffices to show that if $u \in R - P$ and $r \notin Q$, then $u \notin \sqrt{(Q :_R r)}$. Suppose not, in which case $ru^t \in Q$ for some t. Since $u \notin P$, we have $u^t \notin P$, and hence $ru^t \in Q$ implies $r \in Q$ since Q is P-primary, a contradiction.

Finally, the last statement when $r \notin P$ follows similarly: choosing $u \in R - Q$, we want to show that $u \notin (Q :_R r)$. Suppose not, in which case $ru \in Q$. Since $u \notin Q$, we have $r^t \in Q$ for some t, and hence $r \in P$, a contradiction. □

We can now prove the uniqueness of primary decomposition.

Proof of Theorem 8.5.1. (*i*) is part of the definition of irredundancy.

For (*iii*) and (*iv*), we first take radicals to obtain

$$\sqrt{I} = \sqrt{Q_1} \cap \sqrt{Q_2} \cap \cdots \cap \sqrt{Q_n}$$

by Lemma 8.5.2(*i*). We set $P_i = \sqrt{Q_i}$ for every i.

We first show (*iii*). We reorder the Q_i so that $P_1, P_2, \ldots, P_k$ are minimal elements of $\{P_i\}$. We then have

$$\sqrt{I} = P_1 \cap P_2 \cap \cdots \cap P_k,$$

and Lemma 8.5.2(*ii*) implies that the mutually incomparable primes $P_1, P_2, \ldots, P_k$ are the minimal primes of $\sqrt{I}$, and therefore also of I.

We now show (*iv*). Let $P = P_i \in \{P_1, P_2, \ldots, P_k\}$ be one of these minimal primes. Since $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ and finite intersections are compatible with flat base change (Lemma 7.13.4), we see that

$$I_P = (Q_1)_P \cap (Q_2)_P \cap \cdots \cap (Q_n)_P.$$

If $j \neq i$, then $P_j = \sqrt{Q_j}$ is not contained in $P = P_i$, and hence some element $u \in P_j$ is in $R - P$. This element u has a power $u^t \in Q_j$. Therefore, $(Q_j)_P = R_P$. We therefore see that $(Q_i)_P = I_P = IR_P$. Since Q_i is P-primary, if we expand to R_P and then contract, we get Q_i by Proposition 8.2.6(*ii*). Thus, $Q_i = IR_{P_i} \cap R$.

Finally, we show (*ii*). Let $r \in R$. Then,

$$\begin{aligned}
\sqrt{(I :_R r)} &= \sqrt{\big((Q_1 \cap Q_2 \cap \cdots \cap Q_n) :_R r\big)} \\
&= \sqrt{\bigcap_i (Q_i :_R r)} \\
&= \bigcap_i \sqrt{(Q_i :_R r)} \\
&= \bigcap_{\{i \mid r \notin Q_i\}} P_i
\end{aligned}$$

by Lemma 8.5.2(*iii*). Now if $P = \sqrt{(I :_R r)}$ for some $r \in R$, then the intersection on the right-hand side must be equal to one of the P_i, for otherwise the ideal P would not be prime (see Lemma 8.5.2(*ii*)). It remains to show that for every i, there exists an element $r_i \in R$ such that $P_i = \sqrt{(I :_R r_i)}$. First, the intersection of the Q_j for $j \neq i$ cannot be contained in Q_i, for otherwise the decomposition would not be irredundant. Choose

$$r_i \in \left(\bigcap_{j \neq i} Q_j\right) - Q_i.$$

The calculation above shows that $P_i = \sqrt{(I :_R r_i)}$. □

8.6. Associated primes

In the Noetherian case, the primes that appear as radicals in an irredundant primary decomposition have an alternative characterization as *associated* primes. We write down the definition below.

[Rei95, pp. 98–99]
[Hoc17, p. 110]

DEFINITION 8.6.1. A prime ideal $P \subseteq R$ is an *associated prime* of an R-module M if, equivalently,

(1) There is an element $u \in M$ such that $\operatorname{Ann}_R(u) = P$.
(2) There is an injection $R/P \hookrightarrow M$.

The two conditions are equivalent since the submodule of M generated by u is isomorphic to R/P if and only if the annihilator of u in M is equal to P. Note that

an element u for which $\operatorname{Ann}_R(u)$ is prime can never be zero, since $\operatorname{Ann}_R(0) = R$, which is not prime.

The set of associated primes of M is denoted $\operatorname{Ass}_R(M)$, and is also called the set of *assassins* of M.

We will see that in the Noetherian case $\operatorname{Ass}_R(M)$ is finite, and nonempty if $M \neq 0$. It will also turn out that $\operatorname{Ass}_R(R/I)$ is the same as the set of primes that occur as radicals of primary ideals in an irredudant primary decomposition of I. We can see this already in the following:

EXAMPLE 8.6.2. Let $n \in \mathbf{Z}$ be such that $n = p^\alpha q^\beta$ for primes $p \neq q$. Then, the $\mathbf{Z}$-module $\mathbf{Z}/(n)$ has [Rei95, p. 99]

$$\operatorname{Ass}_{\mathbf{Z}}\big(\mathbf{Z}/(n)\big) = \big\{(p), (q)\big\}.$$

Letting $m = p^{\alpha-1}q^\beta$ and setting $\bar{m}$ to be the image of m in $\mathbf{Z}/(n)$, we have $\operatorname{Ann}_{\mathbf{Z}}(\bar{m}) = (p)$, and similarly for q. Also, $\mathbf{Z}/(\ell) \subseteq \mathbf{Z}/(n)$ is only possible if $\ell \mid n$, so no other primes are possible.

The primary decomposition in this case is $(n) = (p^\alpha) \cap (q^\beta)$. This shows that primary decomposition and associated primes both extend the idea of unique factorizations in some sense.

The following fact holds without Noetherian hypotheses. 10/30

PROPOSITION 8.6.3. *Let R be a ring.* [Rei95, p. 99] [Hoc17, p. 110]

(*i*) *If P is a prime ideal in R, then $\operatorname{Ass}_R(R/P) = \{P\}$.*
(*ii*) *If $0 \to M' \to M \to M'' \to 0$ is exact, then*

$$\operatorname{Ass}_R(M) \subseteq \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'').$$

Proof. For (*i*), given any nonzero element $r \in R/P$, choosing a representative $\tilde{r} \in R$ for r, we see that its annihilator is exactly P: if $s \notin P$, then $rs \neq 0$ in R/P.

For (*ii*), we first identify M' with image in M and M'' with the quotient module M/M' to simplify notation. Suppose that $u \in M$ has $\operatorname{Ann}_R(u) = P$, in which case $R/P \simeq R \cdot u \subseteq M$. There are two cases:

(1) If $R \cdot u \cap M' \neq \emptyset$, then some nonzero multiple $v = ru$ of u lies in M', and the annihilator of v is P by the argument in (*i*).
(2) If $R \cdot u \cap M' = \emptyset$, then $R/P \simeq R \cdot u$ embeds into $M/M' = M''$, and hence $P \in \operatorname{Ass}_R(M'')$. □

Our next goal is to show that in the Noetherian case, $\operatorname{Ass}_R(M)$ is nonempty.

LEMMA 8.6.4. *Let M be an R-module, and let $u \in M - \{0\}$. Suppose that either M or R is Noetherian. Then, there exists $r \in R$ such that $ru \neq 0$ and $P = \operatorname{Ann}_R(ru)$ is maximal among ideals that are annihilators of nonzero multiples of u. For such a choice of r, P is a prime ideal.* [Rei95, p. 99] [Hoc17, p. 111]

Proof. First, we may replace M by $R \cdot u$ and R by $R/\operatorname{Ann}_R(M)$ to assume that both M and R are Noetherian (see Proposition 6.2.7). Consider the set of ideals

$$\big\{\operatorname{Ann}_R(ru) \,\big|\, r \in R,\ ru \neq 0\big\}.$$

This is a nonempty family of ideals in a Noetherian ring, and hence there exists an element $ru \in R \cdot u - \{0\}$ such that $\operatorname{Ann}_R(ru)$ is maximal in this set. It remains to show that $P = \operatorname{Ann}_R(ru)$ is prime. Suppose $xy \in P$, but $x \notin P$. Then, $xru \neq 0$, but every element in $P + (y)$ kills xru. By maximality of P, we have $P = P + (y)$, and hence $y \in P$. □

This already implies that in the Noetherian case we have $M = 0$ if and only if $\mathrm{Ass}_R(M) = \emptyset$. On the other hand, this can fail in the non-Noetherian case.

[Hoc17, p. 115] EXAMPLE 8.6.5. Let k be a field, and consider

$$R = \frac{K[X_1, X_2, \ldots,]}{(X_t^{t+1})_{t\geq 1}}.$$

The ideal $\mathfrak{m} = (x_1, x_2, \ldots)$ generated by the images of the X_t is maximal, since the quotient $R/\mathfrak{m}$ is isomorphic to K. Since every x_t is nilpotent, this maximal ideal is also the unique minimal prime of R, and we have $\mathrm{Spec}(R) = \{\mathfrak{m}\}$.

We claim that $\mathrm{Ass}_R(R) = \emptyset$. Since $\mathfrak{m}$ is the only prime ideal of R, it suffices to show that no element of $R - \{0\}$ is killed by $\mathfrak{m}$. Let $f \in R - \{0\}$, and write f as a finite K-linear combination of monomials $x_1^{k_1} \cdots x_n^{k_n}$, such that $0 \leq k_t \leq t$ for every t. If x_N does not appear in this linear combination, then $x_N f \neq 0$, which shows that f is not killed by $\mathfrak{m}$.

8.7. Prime cyclic filtrations and dévissage

We will show something a bit stronger about how many prime ideals can be associated to M.

[Hoc17, p. 111] DEFINITION 8.7.1. Let M be an R-module. A *finite ascending filtration* of M is a sequence

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

of submodules of M. The filtration is said to have *length* n. The modules M_{i+1}/M_i for $i \in \{0, 1, \ldots, n-1\}$ are called the *factors* of the filtration.

We note that if N is a submodule of M, giving a finite ascending filtration of M that contains N is equivalent to that of giving such filtrations for N and M/N: Given filtrations

$$0 = M_0 \subseteq \cdots \subseteq M_k = N \qquad \text{and} \qquad 0 \subseteq M_{k+1}/N \subseteq \cdots \subseteq M_n/N = M/N$$

of N and M/N, respectively, the submodules of M/N correspond bijectively with the submodules of M containing N in such a way that Q/N corresponds to its inverse image Q in M. We can therefore put these filtrations together to obtain

$$0 = M_0 \subseteq \cdots \subseteq M_k \subseteq M_{k+1} \subseteq \cdots \subseteq M_n = M.$$

The factors from this filtration are the union of the two sets of factors for N and M/N, and the length of this filtration for M is the sum of the lengths of the filtrations for N and M/N.

This observation leads to the following:

[Hoc17, p. 111] PROPOSITION 8.7.2. *Let $0 = M_0 \subseteq \cdots \subseteq M_i \subseteq \cdots \subseteq M_n = M$ be a finite ascending filtration of an R-module M. Then,*

$$\mathrm{Ass}_R(M) \subseteq \bigcup_{i=0}^{n-1} \mathrm{Ass}_R(M_{i+1}/M_i).$$

Proof. We proceed by induction on n. If $n = 0$, then there is nothing to show. If $n > 0$, then we consider the short exact sequence $0 \to M_{n-1} \to M \to M/M_{n-1} \to 0$ given by the last part of the filtration. By Proposition 8.6.3(*ii*), we then have

$$\mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(M_{n-1}) \cup \mathrm{Ass}(M/M_{n-1}),$$

and by inductive hypothesis applied to the filtration $0 = M_0 \subseteq \cdots \subseteq M_{n-1}$ for M_{n-1}, we are done. □

We can now describe the associated primes of a Noetherian module M. They will come from the following:

DEFINITION 8.7.3. Let R be a ring. A *cyclic* module is a module generated by a single element. A *prime cyclic* module is a cyclic module with prime annihilator P, which will then be isomorphic to R/P. A *prime cyclic filtration* of an R-module M is a finite ascending filtration in which the factors are prime cyclic modules R/P_i. [Hoc17, p. 112]

THEOREM 8.7.4. *Every Noetherian module $M \neq 0$ has a prime cyclic filtration. We therefore have $\mathrm{Ass}_R(M) \subseteq \{P_1, P_2, \ldots, P_n\}$, and in particular, $\mathrm{Ass}_R(M)$ is finite. Moreover, $\mathrm{Ass}_R(M) = \emptyset$ if and only if $M = 0$.* [Rei95, p. 103] [Hoc17, p. 112]

Proof. By Noetherian induction, we may assume that the result holds for every quotient of M by a nonzero submodule. (If M is a counterexample, the family of submodules N of M such that M/N is a counterexample is nonempty, since it contains 0, and therefore has a maximal element N_1. We then work with M/N_1 instead of M.) Now if $M \neq 0$, we can choose $u \neq 0$ in M and r as in Lemma 8.6.4, in which case $P = \mathrm{Ann}_R(ru)$ is prime. We then have $R/P \simeq R \cdot ru \subseteq M$ and $P \in \mathrm{Ass}_R(M)$. Let $N = R \cdot ru$. By the hypothesis of the Noetherian induction, we know that M/N has a prime cyclic filtration. □

REMARK 8.7.5. The procedure of replacing M by a prime cyclic filtration of M is called *dévissage* in French, which Reid translates to *disassembly*. [Rei95, p. 103]

While all associated primes of a Noetherian module appears in a prime cyclic filtration, it may be impossible to give a prime cyclic filtration such that only the primes in $\mathrm{Ass}_R(M)$ appear.

EXAMPLE 8.7.6. Let R be a domain, and let M be a torsion-free R-module. Then, $\mathrm{Ann}_R(u) = (0)$ for every nonzero element $u \in M$, and hence $\mathrm{Ass}_R(M) = \{(0)\}$. [Hoc17, p. 115]

Now suppose that M is torsion-free but not free (for example, we saw that $(2, x) \subseteq \mathbf{Z}[x]$ is torsion-free but not free in Example 2.2.14). We claim that a prime cyclic filtration cannot consist of factors that are isomorphic to $R = R/(0)$. It suffices to show that if M has such a filtration, then M would be free. This is clear if the filtration is of length 1, and otherwise, there is a surjection $M \twoheadrightarrow R$ onto the last factor, which splits since R is free, hence projective; the torsion-free module $M_{n-1} \simeq M/R$ has a filtration of length one smaller, and hence is free by inductive hypothesis.

In the explicit example of Example 2.2.14, we have for example the prime cyclic filtration

$$0 \subseteq (2) \subseteq (2, x),$$

where $(2)/(0) \cong \mathbf{Z}[x]$ and $(2, x)/(2) \cong x \cdot \mathbf{F}_2[x]$.

8.8. Behavior under localization

Before we establish the connection between primary decomposition and associated primes and give applications, we need to understand how both notions behave under localization.

We start with associated primes. One reason to expect that associated primes behave well is that prime cyclic filtrations behave well under localization. We need to work a bit harder to show that $\mathrm{Ass}_R(M)$ itself is compatible with localization.

11/1

PROPOSITION 8.8.1. *Let M be an R-module, and let $W \subseteq R$ be a multiplicative subset. We then have*

[Hoc17, p. 112]
[BouCA, Prop. IV.1.5]

$$\mathrm{Ass}_{W^{-1}R}(W^{-1}M) \supseteq \left\{ P \cdot W^{-1}R \;\middle|\; P \in \mathrm{Ass}_R(M) \text{ and } P \cap W = \emptyset \right\},$$

and equality holds if R is Noetherian. More precisely, if $P \subseteq R$ is a finitely generated prime ideal, then $P \cdot W^{-1}R \in \mathrm{Ass}_{W^{-1}R}(W^{-1}M)$ if and only if $P \in \mathrm{Ass}_R(M)$ and $P \cap W = \emptyset$.

Proof. For the inclusion $\supseteq$, it suffices to note that an injection $R/P \hookrightarrow M$ localizes to an inclusion

$$\frac{W^{-1}R}{P \cdot W^{-1}R} \cong W^{-1}(R/P) \longhookrightarrow W^{-1}M,$$

and the assumption that $P \cap W = \emptyset$ is used to show that $P \cdot W^{-1}R$ is prime.

Now suppose $P = (f_1, f_2, \ldots, f_s)$ is finitely generated and that $P \cdot W^{-1}R \in \mathrm{Ass}_{W^{-1}R}(W^{-1}M)$. By definition, there exists a nonzero element of $W^{-1}M$ such that $P \cdot W^{-1}R$ is its annihilator. After multiplying such an element by an element in the image of W, we may assume that this element is of the form $u/1$ for $u \in M - \{0\}$. Since $f_i u/1 = 0$ in $W^{-1}M$ for every i, for every i we can choose $w_i \in W$ such that $w_i f_i u = 0$. Let $w = w_1 w_2 \cdots w_s$. We claim that $P = \mathrm{Ann}_R(wu)$. Each of the elements $f_1, f_2, \ldots, f_s$ kill wu, and hence P kills wu, showing $\subseteq$. Conversely, suppose $r \in R$ satisfies $rwu = 0$. Then, $r/1 \in P \cdot W^{-1}R$ by definition, and hence $r \in P$. Thus, $P = \mathrm{Ann}_R(wu)$ and $P \in \mathrm{Ass}_R(M)$. □

This is another property that does not work well for non-Noetherian rings.

[Hoc17, p. 115]

EXAMPLE 8.8.2. Let K be a field, and consider the polynomial ring $R = K[y, x_1, x_2, \ldots]$ in countably many variables. Let $P = (x_i)_{i \geq 1}$, and let $M = R/J$ where $J = (y^i x_i)_{i \geq 1}$. Let $W = \{y^t \mid t \geq 0\}$. Then,

$$P \cdot W^{-1}R \in \mathrm{Ass}_{W^{-1}R}(W^{-1}M)$$

since $W^{-1}M \cong W^{-1}R/P \cdot W^{-1}R$. On the other hand, no element of $R - J$ is multiplied into J by P, and hence $P \notin \mathrm{Ass}_R(M)$.

[Hoc17, p. 112]

COROLLARY 8.8.3. *Let M be a finitely generated module over a Noetherian ring, and suppose that $\mathrm{Ass}_R(M) = \{P_1, P_2, \ldots, P_n\}$. Then,*

$$\sqrt{\mathrm{Ann}_R(M)} = \bigcap_i P_i.$$

Thus, $\sqrt{\mathrm{Ann}_R(M)}$ is the intersection of minimal elements of $\mathrm{Ass}_R(M)$, which coincide with the minimal primes of $\sqrt{\mathrm{Ann}_R(M)}$ and also of $\mathrm{Ann}_R(M)$.

Proof. Let $u_1, u_2, \ldots, u_h$ generate M. Let $r \in R$. We know that $u_i/1 = 0$ in $M_r = W^{-1}M$, where $W = \{1, r, r^2, \ldots\}$, if and only if some power of r kills u_i. We

now have the following sequence of equivalences:

$$\begin{aligned} M_r = 0 &\iff \frac{u_i}{1} = 0 \text{ in } M_r \text{ for every } i \\ &\iff \text{for every } i, \text{ there exists an } n_i \text{ such that } r^{n_i} u_i = 0 \\ &\iff \text{there exists an } n \text{ such that } r^n u_i = 0 \text{ for every } i \\ &\iff r \in \sqrt{\operatorname{Ann}_R(M)}. \end{aligned}$$

But $M_r = 0$ if and only if $\operatorname{Ass}_{R_r}(M_r) = \emptyset$, and $\operatorname{Ass}_{R_r}(M_r)$ is the set of primes in $\operatorname{Ass}_R(M)$ not containing r, so that $M_r = 0$ if and only if r is in every prime in $\operatorname{Ass}_R(M)$. □

Finally, we show that primary decompositions behave well under localization. We need the following:

LEMMA 8.8.4. *If J is an ideal in a ring R, then* [Hoc17, p. 113]

$$\sqrt{J \cdot W^{-1}R} = \sqrt{J} \cdot W^{-1}R.$$

Proof. It suffices to show $\subseteq$. If u/w_0 has a power in $JW^{-1}R$, where $u \in R$ and $w_0 \in W$, then $u/1$ does as well, and hence $u^n/1 = j/w_1$ for some $n \in \mathbf{N}$, $j \in J$, and $w_1 \in W$. It therefore follows that for some $w_1 \in W$, we have

$$w_2(w_1 u^n - j) = 0,$$

from which we see that $wu^n \in J$ where $w = w_1 w_2$, and hence $(wu)^n \in J$ as well. Then, $u \in \sqrt{J} \cdot W^{-1}R$. □

PROPOSITION 8.8.5. *Let R be a ring, and suppose that I has an irredundant primary decomposition* [Hoc17, p. 113]

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

and denote $P_i = \sqrt{Q_i}$. Let W be a multiplicative subset in R. Then the intersection of the $Q_i \cdot W^{-1}R$ such that P_i does not meet W is an irredundant primary decomposition of $I \cdot W^{-1}R$. In particular, if Q is primary with radical P, then

$$Q \cdot W^{-1}R = \begin{cases} W^{-1}R & \text{if } W \cap P \neq \emptyset; \\ \text{primary to } P \cdot W^{-1}R & \text{otherwise.} \end{cases}$$

Proof. We first show the last statement. If W meets P, then some element of W has a power in Q, and so $Q \cdot W^{-1}R = W^{-1}R$. If not, $QW^{-1}R$ has radical $PW^{-1}R$ by the previous Lemma, and it suffices to show that if $r, s \in R$, $v, w \in W$, and $(r/v)(s/w) \in Q \cdot W^{-1}R$, then $r/w \in Q \cdot W^{-1}R$ or $s/w \in \sqrt{Q \cdot W^{-1}R}$. Since

$$\frac{r}{v} \cdot \frac{s}{w} = \frac{rs}{vw} \in Q \cdot W^{-1}R,$$

we see that $w'(rs) \in Q$ for some $w' \in W$. Since $W \subseteq R - P$, this implies that $rs \in Q$, so $r \in Q$ or $s \in \sqrt{Q}$, from which the desired result follows.

We now show the statement about primary decompositions. Since localization commutes with finite intersection, we have $W^{-1}I = \bigcap_i W^{-1}Q_i$, and hence we may take out the terms such that W meets P, since for these terms, $W^{-1}Q_i$ is the unit ideal. This gives a primary decomposition involving distinct primes. To see it is

irredundant, let P_i be a fixed one of the primes occurring that is disjoint from W. We know that $P_i = \sqrt{(I :_R r)}$ for some element $r \in R$. Then,

$$\begin{aligned} W^{-1}P_i &= W^{-1}\Big(\sqrt{(I :_R r)}\Big) \\ &= \sqrt{W^{-1}(I :_R r)} \\ &= \sqrt{\big(W^{-1}I :_{W^{-1}R} (r/1)\big)}, \end{aligned}$$

which, by our earlier criterion for when a prime must occur as the radical of some term in a primary decomposition, shows that all of the terms are needed. □

8.9. Primary decomposition and associated primes

We now connect primary decompositions and associated primes.

[Hoc17, p. 117]

THEOREM 8.9.1. *Let R be a Noetherian ring, M an R-module, and let $I \subseteq R$ be an ideal.*

- (*i*) *An element $r \in R$ is a zerodivisor on M (i.e., $ru = 0$ for some $u \in M - \{0\}$) if and only if $r \in P$ for some $P \in \operatorname{Ass}_R(M)$. In other words, the set of zerodivisors on M in R is the same as the union of associated prime ideals of M.*
- (*ii*) *I is primary if and only if $\operatorname{Ass}_R(R/I)$ contains just one element P, in which case I is primary to P.*
- (*iii*) *The primes appearing as radicals of primary ideals appearing in an irredundant primary decomposition for I are the elements of $\operatorname{Ass}_R(R/I)$.*

Proof. For (*i*), we first show $\Leftarrow$. If $r \in P \in \operatorname{Ass}_R(M)$, then there exists $u \in M - \{0\}$ such that $P = \operatorname{Ann}_R(u)$, and we have $ru = 0$. Conversely, if $ru = 0$ with $u \neq 0$, then u has a multiple $r'u$ that is not zero with prime annihilator P by Lemma 8.6.4. We then see that $rr'u = 0$.

For (*ii*), we note that if I is primary, then the zerodivisors on I are precisely the elements of P/I: the elements of P/I are nilpotent on I, and are therefore zerodivisors, and conversely, the elements of $R - P$ are not zerodivisors on the module R/I by Proposition 8.2.6(*iii*).

We now show $\Rightarrow$ in (*iii*). Let $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ be an irredundant primary decomposition of I, and set $P_i = \sqrt{Q_i}$ for every i. We then have

$$\frac{R}{I} \hookrightarrow \bigoplus_i \frac{R}{Q_i},$$

and hence

$$\operatorname{Ass}_R(R/I) \subseteq \bigcup_i \operatorname{Ass}_R(R/Q_i) = \{P_1, P_2, \ldots, P_n\}$$

by the previous paragraph. It remains to show the converse. Fix i and choose $r \in R$ such that $\sqrt{(I :_R r)} = P_i$. Let

$$N = \frac{I + rR}{I} \cong \bar{r} \cdot \frac{R}{I}.$$

Then, $\operatorname{Ass}_R(N) \subseteq \operatorname{Ass}_R(R/I)$. But $\operatorname{Ann}_R(N) = (I :_R r)$ whose radical is P_i. Since P_i is a minimal prime of $\operatorname{Ann}_R(N)$, we see that

$$P_i \in \operatorname{Ass}_R(N) \subseteq \operatorname{Ass}_R(R/I)$$

by Corollary 8.8.3.

Finally, we show the direction $\Leftarrow$ in (*ii*). If $\operatorname{Ass}_R(R/I)$ contains just one element P, then (*iii*) shows that there is only one term in the primary decomposition of I with $P = \sqrt{I}$. □

Remark 8.9.2. Theorem 8.9.1 suggests that there is a theory of primary decomposition for modules. This is indeed the case; see [Hoc17, pp. 119–120] for a precise statement. This is the approach taken by Bourbaki [BouCA, Chapter IV, §2].

Before we move on, we want to state one open problem about associated primes.

Example 8.9.3 [NB14, p. 771]. For $n \geq 4$, consider the ring

$$R = \frac{\mathbf{Z}_p[\![x, y, z_1, \dots, z_n]\!]}{(p - xy)}.$$

Is it true that for every finite set $f_1, f_2, \dots, f_m \in R$, the set of associated primes of

$$H^m_{(f_1,f_2,\dots,f_m)}(R) \coloneqq \frac{R_{f_1 f_2 \cdots f_m}}{\sum_j R_{f_1 \cdots \widehat{f_j} \cdots f_m}}$$

is finite? The case $n < 4$ is known by [Mar01, Corollary 2.10] since $\dim(R) \leq 4$.

8.10. Krull's intersection theorem

We now want to apply our theory of primary decomposition. The first result is a special case of Krull's intersection theorem.

Theorem 8.10.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then, $\bigcap_j \mathfrak{m}^j = (0)$.* [Hoc17, p. 117]

Proof. Let $J = \bigcap_j \mathfrak{m}^j$. Let $\mathfrak{m}J = Q_1 \cap \cdots \cap Q_n$ be a primary decomposition for $\mathfrak{m}J$. We will show that $J \subseteq Q_i$ for every i. This would then show that $J \subseteq \mathfrak{m}J$, in which case $J = \mathfrak{m}J$, and the NAK lemma would then show that $J = (0)$.

To prove $J \subseteq Q_i$, we consider two cases.

(1) If $P_i = \sqrt{Q_i} \neq \mathfrak{m}$, choose $x \in \mathfrak{m} - P_i$. Then, $xJ \subseteq \mathfrak{m}J \subseteq Q_i$, but $x \notin \sqrt{Q_i}$. This shows that $J \subseteq Q_i$ by the definition of primariness.
(2) If $P_i = \sqrt{Q_i} = \mathfrak{m}$, then every generator of $\mathfrak{m}$ has a power in Q_i, and since $\mathfrak{m}$ is finitely generated, $\mathfrak{m}^N \subseteq Q_i$ for all sufficiently large N by the pigeon-hole principle. But $J \subseteq \mathfrak{m}^N$ for all N, and hence $J \subseteq Q_i$. □

8.11. Artinian rings are Noetherian

Our next goal is to prove that Artinian rings are always Noetherian.

8.11.1. A version of primary decomposition for non-Noetherian rings. To do so, we have to prove one version of primary decomposition for non-Noetherian rings.

Theorem 8.11.1. *Let R be any ring and let I be an ideal such that $V(I)$ is a finite set of ideals, all of which are maximal. Then, I has a primary decomposition* [Hoc17, p. 121]

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

which is unique except for the order of terms. In this case, $I = \prod_i Q_i$, and

$$\frac{R}{I} \cong \prod_{i=1}^{n} \frac{R}{Q_i}.$$

Proof. It is equivalent to find a primary decomposition for (0) in R/I. Therefore we may assume that R is a ring such that every prime ideal is maximal, and where there are only finitely many maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n$. Let Q_i be the contraction of $(0) \subseteq R_{\mathfrak{m}_i}$ under the localization map $R \to R_{\mathfrak{m}_i}$. Then, since $(0) \subseteq R_{\mathfrak{m}_i}$ is $\mathfrak{m}_i R_{\mathfrak{m}_i}$-primary, we see that Q_i is $\mathfrak{m}_i$-primary in R. Moreover, we have

$$0 = Q_1 \cap Q_2 \cap \cdots \cap Q_n,$$

since any element of this intersection vanishes no matter at which prime ideal R we localize, and the property of being the zero module is local. This gives a primary decomposition of (0), which is unique since all primes occurring as radicals are maximal, and hence are all minimal in the set of primes occurring in the decomposition.

Since the Q_i have radicals that are mutually distinct maximal ideals, they are pairwise comaximal: if $i \neq j$, then

$$\sqrt{Q_i + Q_j} \supseteq \sqrt{Q_i} + \sqrt{Q_j} = \mathfrak{m}_i + \mathfrak{m}_j = R \implies Q_i + Q_j = R,$$

and the rest follows from the Chinese Remainder Theorem 4.5.5. □

11/4

8.11.2. Length. To show that Artinian rings are Noetherian, it is convenient to introduce the notion of *length*.

[Hoc17, p. 121]

Definition 8.11.2. A nonzero module over a ring R is *simple* if, equivalently,

(1) It has no nonzero proper submodule; or
(2) It is isomorphic to $R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

Any module satisfying (1) is generated by any nonzero element, and is therefore cyclic and of the form R/I for some proper ideal I. The assumption that there are no nonzero proper submodules means that every nonzero ideal must be the unit ideal, which forces R/I to be a field.

A module has *finite length* if it has a filtration in which every factor is simple. The *length* $\ell_R(M)$ of an R-module M is then defined to be the number of simple factors in any finite filtration such that all factors are simple or zero.

[Hoc17, pp. 121–122]

Lemma 8.11.3. *The length of a module is well-defined, and is additive on short exact sequences.*

Proof. The well-definedness is a consequence of the (module version of the) Jordan–Hölder theorem from abstract algebra. See, for example, [ZS75, Chapter III, §11, Theorem 19] or [AK21, (19.3)]. The additivity on short exact sequences follows by what we said when we discussed filtrations on p. 132: we can take filtrations on $M' \subseteq M$ and on M/M' to give a filtration on M. □

As a consequence of Lemma 8.11.3, finite length modules have both ACC and DCC: An infinite ascending or descending chain would necessarily mean that the length is infinite, since each factor contributes positively to the length.

Over fields, being of finite length is *equivalent* to having ACC or DCC.

[Hoc17, p. 122]

Example 8.11.4. For a vector space W over a field k, the conditions of W having ACC, DCC, being of finite length, and having finite k-dimension are all equivalent. By what we said above, it suffices to show that having ACC or DCC imply that W has finite length. If W has ACC (resp. DCC), then we can find an ascending (resp. descending) chain of subspaces of W that increases (resp. decreases)

the cardinality of a basis one at a time. By ACC (resp. DCC), such a sequence must stabilize. Since each factor of the filtration has dimension 1 over k, we see that W has finite length by Lemma 8.11.3.

More generally, if M is a module over a local ring $(R, \mathfrak{m})$ such that $\mathfrak{m} \cdot M = 0$, then

$$\ell_R(M) < \infty \iff \dim_{R/\mathfrak{m}}(M) < \infty.$$

This is because each simple factor is isomorphic to $R/\mathfrak{m}$ by characterization (2) of being a simple module in Definition 8.11.2, and hence the length of the filtration is equal to the $R/\mathfrak{m}$-vector space dimension.

Over a PID R, the length of $R/(f)$ is the same as the number n of irreducible factors in a factorization

$$f = f_1 f_2 \cdots f_n$$

counted with multiplicity. This follows from the Chinese Remainder Theorem 4.5.5 where if g is irreducible, we note that

$$\frac{R}{(g^n)} \supseteq \frac{g}{g^n} \supseteq \frac{g^2}{g^n} \supseteq \cdots \supseteq \frac{g^{n-1}}{g^n} \supseteq 0$$

is a finite filtration of length n with factors $g^i/g^{i+1} \cong R/(g)$. Thus,

$$\ell_{\mathbf{Z}}\left(\frac{\mathbf{Z}}{60\mathbf{Z}}\right) = 4$$

since $60 = 2 \cdot 2 \cdot 3 \cdot 5$ and

$$\ell_{k[x]}\left(\frac{k[x]}{(x^3 - x)}\right) = 3$$

since $x^3 - x = (x-1)x(x+1)$.

For Noetherian modules, we can describe lengths as follows:

LEMMA 8.11.5. *Let M be an R-module. Then, M has finite length if and only if M is Noetherian and $\mathrm{Ass}_R(M)$ consists only of maximal ideals.* [Hoc17, p. 122]

Proof. $\Rightarrow$. Each factor in a finite filtration with simple factors is prime cyclic of the form $R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m} \subseteq R$. Thus, M is Noetherian and $\mathrm{Ass}_R(M)$ consists only of maximal ideals.

$\Leftarrow$. Replacing R by $R/\mathrm{Ann}_R(M)$, we may assume that R is Noetherian. If M is Noetherian and $\mathrm{Ass}_R(M)$ consists only of maximal ideals, then $\sqrt{\mathrm{Ann}_R(M)}$ is the intersection of these maximal ideals by Corollary 8.8.3. Any prime occurring in the finite prime cyclic filtration for M must contain $\sqrt{\mathrm{Ann}_R(M)}$ and therefore lies in $\mathrm{Ass}_R(M)$. It follows that the only factors in the finite prime cyclic filtration are of the form $R/\mathfrak{m}$ where $\mathfrak{m} \subseteq R$ is a maximal ideal. □

LEMMA 8.11.6. *A Noetherian local ring $(R, \mathfrak{m}, k)$ of Krull dimension 0 has finite length as a module over itself.* [Hoc17, p. 122]

Proof. Since $\mathfrak{m}$ is nilpotent and finitely generated, there is a power $\mathfrak{m}^n$ of $\mathfrak{m}$ such that $\mathfrak{m}^n = (0)$. We then have a filtration

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m}^2 \subseteq \mathfrak{m} \subseteq R$$

is a filtration of R. Each factor is of the form $\mathfrak{m}^i/\mathfrak{m}^{i+1}$, which is a finite-dimensional vector space over $R/\mathfrak{m}$ since $\mathfrak{m}^i$ is finitely generated. We then have

$$\ell_R(R) = \sum_{i=0}^{n-1} \dim_{R/\mathfrak{m}}(\mathfrak{m}^i/\mathfrak{m}^{i+1}) < \infty. \qquad \square$$

8.11.3. Artinian rings are Noetherian. We can now show:

[Hoc17, p. 122]

THEOREM 8.11.7 (Akizuki [Aki35]). *Let R be a ring. The following are equivalent:*

(*i*) *R is Noetherian of Krull dimension zero.*
(*ii*) *R is a finite product of Noetherian local rings of Krull dimension zero.*
(*iii*) *R has finite length as a module over itself.*
(*iv*) *R has DCC, i.e., R is Artinian.*

Proof. (*i*) $\Rightarrow$ (*ii*). All prime ideals of R are minimal as well as maximal. Thus, R has only finitely many maximal ideals $\mathfrak{m}_i$, and we may use Theorem 8.11.1 to write (0) as a finite product of $\mathfrak{m}_i$-primary ideals.

(*ii*) $\Rightarrow$ (*iii*) follows from Lemma 8.11.6.

(*iii*) $\Rightarrow$ (*iv*) holds since modules of finite length have DCC.

It remains to show that (*iv*) $\Rightarrow$ (*i*). We proceed in a few steps:

STEP 1. $\dim(R) = 0$.

Let P be a prime ideal in R, and consider the ring $A = R/P$, which also has DCC. Choose $a \in A - \{0\}$. We claim that a is a unit. The sequence of ideals (a^n) must stabilize by DCC. But then, $a^n \in (a^{n+1})$ for some n, and hence there exists $b \in A$ such that $a^n = a^{n+1}b$. Since $a \neq 0$ and A is a domain, this shows $1 = ab$. We therefore see that every prime ideal in R is maximal.

STEP 2. There are only finitely many maximal ideals $\mathfrak{m}_i$ in R.

If there are infinitely many, then the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots$$

would have to stabilize, yielding $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ for some large n. But then, $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_i$ for some $i \leq n$ by Lemma 8.5.2(*ii*), a contradiction.

STEP 3. We may assume that R is local with a unique prime ideal.

Theorem 8.11.1 implies that we can write (0) as a finite product of $\mathfrak{m}_i$-primary ideals and that R is isomorphic to the direct product of the $R_{\mathfrak{m}_i}$.

STEP 4. An Artinian local ring $(R, \mathfrak{m}, k)$ is Noetherian.

We then have the chain of ideals

$$R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots.$$

This chain of ideals eventually stablizes at $\mathfrak{m}^n$. We know that each factor $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a finite-dimensional k-vector space by Lemma 6.2.5(*iii*) since it is a subquotient of R. It therefore remains to show that $\mathfrak{m}^n = 0$. Suppose not. Consider the family of ideals

$$\Sigma = \left\{ I \subseteq \mathfrak{m} \;\middle|\; I \cdot \mathfrak{m}^n \neq 0 \right\}.$$

Then, $\mathfrak{m} \in \Sigma$. By the DCC condition, there exists a minimal member $J \in \Sigma$. By definition, there exists $x \in J$ such that $x \cdot \mathfrak{m}^n \neq 0$, and hence $xR \in \Sigma$. By minimality, $J = xR$. Then,

$$x \cdot \mathfrak{m} \cdot \mathfrak{m}^n = x \cdot \mathfrak{m}^{n+1} = x \cdot \mathfrak{m}^n \neq 0,$$

and hence $x \cdot \mathfrak{m} \subseteq xR \in \Sigma$. By minimality, $xR = x \cdot \mathfrak{m} = \mathfrak{m} \cdot xR$. By NAK, $xR = 0$, a contradiction. Thus, $\mathfrak{m}^n = 0$, and hence R has a finite filtration

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m}^2 \subseteq \mathfrak{m} \subseteq R$$

whose factors are finite-dimensional k-vector spaces. Thus, R has finite length as a module over itself, and is therefore Noetherian. □

8.12. Krull's height theorem and systems of parameters

Our next goal is to use primary decomposition to prove some things about the behavior of dimension for Noetherian rings. We start with the following result, which is originally due to Krull. A historical note: This proof is where Krull introduced symbolic powers. According to Hochster, it was surprising at the time that Noetherianity is all one needs for this result to hold.

THEOREM 8.12.1 (Krull's principal ideal theorem [Kru38, Satz 7* on p. 220]). *Let R be a Noetherian ring, $x \in R$, and P a minimal prime of $(x) \subseteq R$. Then,* [AK21, (21.10)] [Hoc17, p. 124] [AM69, Cor. 11.17]

$$\operatorname{ht}(P) \leq 1.$$

Proof. We proceed by contradiction. Suppose we have a chain

$$Q_0 \subsetneq Q \subsetneq P,$$

where P is minimal over (x), and hence $x \notin Q$. We can replace R by R_P/Q_0R_P to get a counterexample where R is a local domain (R, P) and P is minimal over (x).

Recall the n-th symbolic power of Q is

$$Q^{(n)} \coloneqq Q^n R_Q \cap R,$$

which is a Q-primary ideal by Proposition 8.2.7(*ii*). The ring $R/(x)$ has only one prime ideal $P/(x)$, since P is a maximal ideal in R minimal over (x) by the reduction in the previous paragraph. Therefore it is a 0-dimensional Noetherian local ring, and has DCC. Thus, the chain of ideals $Q^{(n)}/(x)$ is eventually stable. Taking preimages in R, we find that there exists N such that

$$Q^{(n)} + (x) = Q^{(n+1)} + (x)$$

for all $n \geq N$. We therefore have

$$Q^{(n)} \subseteq Q^{(n+1)} + (x).$$

STEP 1. $Q^{(n)} = Q^{(n+1)} + x\,Q^{(n)}$.

Note that it suffices to show the inclusion $\subseteq$, since both ideals on the right-hand side are contained in $Q^{(n)}$. Let $u \in Q^{(n)}$. Write $u = q + xr$ where $q \in Q^{(n+1)}$, in which case $xr = u - q \in Q^{(n)}$ since $u \in Q^{(n)}$ and $q \in Q^{(n+1)} \subseteq Q^{(n)}$. But $x \notin Q$ since P is minimal over (x) in R. Since $Q^{(n)}$ is Q-primary, we have that $r \in Q^{(n)}$. Thus, we have $Q^{(n)} \subseteq Q^{(n+1)} + x\,Q^{(n)}$.

STEP 2. $Q^{(n)} = Q^{(N)}$ for all $n \geq N$

Set $M = Q^{(n)}/Q^{(n+1)}$. The previous step shows that $M = xM$. Nakayama's lemma then implies that $M = 0$, and hence $Q^{(n)}/Q^{(n+1)} = 0$. Thus, $Q^{(n)} = Q^{(N)}$ for all $n \geq N$.

Step 3. $\bigcap Q^n R_Q \neq 0$, contradicting Krull's intersection theorem.

Choose $a \in Q - \{0\}$. Then, $a^N \in Q^N \subseteq Q^{(N)}$, and hence $a^N \in \bigcap_n Q^{(n)}$. But then, the image of a^N in R_Q is contained in $\bigcap_n Q^{(n)} R_Q = \bigcap_n Q^n R_Q$ (here we use [AK21, (1.14)(2)]), and the image of a^N is nonzero since we are localizing a domain at a prime ideal. □

11/6

This is actually enough to prove that dimension works well under faithfully flat maps, which is on Homework 10. We will be a bit more ambitious and prove:

[Hoc17, p. 125] [AM69, Prop. 11.13, Cor. 11.16]

Theorem 8.12.2 (Krull's height theorem [Kru38, Satz 7* on p. 220]). *Let R be a Noetherian ring.*

(*i*) *If $I = (x_1, x_2, \ldots, x_n)$ is an ideal generated by n elements, then* $\operatorname{ht}(P) \leq n$ *for every minimal prime P of I.*

(*ii*) *Conversely, if P is a prime ideal of height n, then it is a minimal prime of an ideal generated by n elements.*

This has some consequences which we state first. Below, R is a Noetherian ring and P is a prime ideal.

(1) The height of P is the least number of generators of an ideal $I \subseteq P$ over which P is a minimal prime.
(2) The height of every prime ideal is at most the number of generators of P, and hence is finite.
(3) Noetherian local rings have finite Krull dimension (this is not the case for non-local rings as you saw on the homework).

Proof of Theorem 8.12.2(i). We proceed by induction on n. The $n = 0$ case is the case when $I = (0)$, and the $n = 1$ case is Theorem 8.12.1. Now suppose P is a minimal prime of $I = (x_1, x_2, \ldots, x_n)$. By way of contradiction, suppose we have a chain of primes

$$P = P_{n+1} \supsetneq \cdots \supsetneq P_0 \tag{8.12.3}$$

of length $n + 1$.

Step 1. It suffices to show that we can modify the chain (8.12.3) so that $x_1 \in P_1$.

If $x_1 \in P_1$, then P is also a minimal prime of $P_1 + (x_2, \ldots, x_n)$. We therefore see that P/P_1 is a minimal prime of $(x_2, \ldots, x_n)/P_1$. Then, the chain

$$P/P_1 = P_{n+1}/P_1 \supsetneq \cdots \supsetneq P_1/P_1 = 0$$

would contradict the inductive hypothesis.

Step 2. If $x_1 \in P_k - P_{k-1}$ for some $k \geq 2$, then there is a prime ideal strictly between P_k and P_{k-2} that contains x_1.

Consider the local domain

$$D = R_{P_k}/P_{k-2}R_{P_k}.$$

The element x_1 has nonzero image in the maximal ideal of D. In this ring, $P_k R_{P_k}$ has height ≥ 2, and hence a minimal prime P' of (x_1) has height ≤ 1 by Theorem 8.12.1, and is strictly contained in $P_k R_{P_k}$. The preimage of P' in R works.

Step 3. We can modify the chain (8.12.3) so that $x_1 \in P_1$.

By applying the previous step repeatedly, we can modify the chain (8.12.3) so that $x_1 \in P_1$. □

Proof of Theorem 8.12.2(ii). We proceed by induction on n. If $n = 0$, then we take the ideal (0) generated by the empty set. The fact that P has height zero means that it is a minimal prime of (0).

Now suppose that $n > 0$. Let $Q_1, Q_2, \ldots, Q_k$ be the minimal primes of R that are contained in P; note there are only finitely many by our first application of Noetherian induction (Theorem 6.4.1). Then, P cannot be contained in $\bigcup_i Q_i$ by the prime avoidance theorem, for otherwise $\operatorname{ht}(P) \leq \operatorname{ht}(Q_i) = 0$ for some i. Choose $x_1 \in P - \bigcup_i Q_i$. Then, the height of $P/(x_1)$ in $R/(x_1)$ is at most $n-1$, since a chain of maximal length must end at a minimal prime in R, and these minimal primes are not available in $R/(x_1)$. By the inductive hypothesis, $P/(x_1)$ is a minimal prime of an ideal generated by at most $n-1$ elements. Consider x_1 together with preimages $x_2, \ldots, x_m$ of each of these elements in R. Then, P is a minimal prime of the ideal $(x_1, x_2, \ldots, x_m)$ generated by at most m elements. The number m cannot be smaller than n, or else by (*i*), we would have that $\operatorname{ht}(P) < n$. □

This gives a useful way to think of the dimension of a local ring.

Definition 8.12.4. Let $(R, \mathfrak{m})$ be a Noetherian local ring of Krull dimension n. A *system of parameters* for R is a sequence of elements $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ such that, equivalently: [AK21, (21.2)] [Hoc17, p. 128] [AM69, p. 122]

(1) $\mathfrak{m}$ is a minimal prime of $(x_1, x_2, \ldots, x_n)$.
(2) $\sqrt{(x_1, x_2, \ldots, x_n)} = \mathfrak{m}$.
(3) $\mathfrak{m}$ has a power in $(x_1, x_2, \ldots, x_n)$.
(4) $(x_1, x_2, \ldots, x_n)$ is $\mathfrak{m}$-primary.

If $\mathfrak{m}$ itself can be generated by a system of parameters, we say that R is a *regular local ring*, in which case the system of parameters is called a *regular system of parameters*.

Theorem 8.12.2(*ii*) in fact shows:

Corollary 8.12.5. *Every Noetherian local ring $(R, \mathfrak{m})$ has a system of parameters.* [Hoc17, p. 128] [AM69, Prop. 11.13]

We write down how to do this in practice, although the proof is just a rewording of the proof of Theorem 8.12.2(*ii*)

Proof. As in the proof of Theorem 8.12.2(*ii*), one begins by choosing $x_1 \in \mathfrak{m}$ avoiding all of the minimal primes of R. Then, $\dim(R/(x_1)) = \dim(R) - 1$ by Theorem 8.12.1 and the argument in the proof of Theorem 8.12.2(*ii*). We then choose $x_2 \in R$ such that its image in $R/(x_1)$ avoids all the minimal primes in $R/(x_1)$. Repeating this process, we eventually end up with a local ring of dimension zero, which happens after $\dim(R)$ steps. □

Corollary 8.12.6. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and let $x_1, x_2, \ldots, x_k \in \mathfrak{m}$. Then, $\dim(R/(x_1, \ldots, x_k)) \geq \dim(R) - k$, and equality holds if $x_1, \ldots, x_k$ are part of a system of parameters.* [AK21, (21.5), (21.6)] [Hoc17, p. 129] [AM69, Cor. 11.18]

Proof. Set $h = \dim(R/(x_1, \dots, x_k))$. If $y_1, y_2, \dots, y_h \in \mathfrak{m}$ have images that are a system of parameters in $R/(x_1, \dots, x_k)$, then $\mathfrak{m}$ is a minimal prime of

$$(x_1, \dots, x_k, y_1, \dots, y_h),$$

and hence $h + k \geq n$.

Now if $x_1, \dots, x_k$ are part of a system of parameters, we can extend them to a system of parameters $x_1, \dots, x_k, y_1, \dots, y_h \in \mathfrak{m}$. The image of $\mathfrak{m}$ in $R/(x_1, \dots, x_k)$ is minimal over $(y_1, \dots, y_h)$, and hence $h \geq \dim(R/(x_1, \dots, x_k))$. We therefore have

$$\dim(R) = h + k \geq \dim(R/(x_1, \dots, x_k)) + k. \qquad \square$$

8.13. Dimension of formal power series rings

Our last goal before moving on to the next topic is to show the formal power series version of one of your homework problems from Homework 7.

[Hoc17, p. 129] LEMMA 8.13.1. *Let x be an indeterminate over R. Then, x is in every maximal ideal of $R[\![x]\!]$.*

Proof. Let $\mathfrak{M}$ be a maximal ideal. If $x \notin \mathfrak{M}$, then x has an inverse modulo $\mathfrak{M}$, and hence we have $xf \equiv 1 \bmod \mathfrak{M}$. This is equivalent to saying that $1 - xf \in \mathfrak{M}$. It therefore suffices to show that $1 - xf$ is a unit. We claim that

$$u = 1 + xf + x^2f^2 + x^3f^3 + \cdots$$

is an inverse. The infinite sum makes sense because only finitely many terms involve any given power of x. Note that

$$u = (1 + xf + \cdots + x^n f^n) + x^{n+1} w_n$$

for

$$w_n = f^{n+1} + xf^{n+2} + x^2 f^{n+3} + \cdots,$$

which again makes sense because only finitely many terms involve any given power of x. Thus,

$$u(1 - xf) - 1 = \underbrace{(1 + xf + \cdots + x^n f^n)(1 - xf)}_{1 - x^{n+1} f^{n+1}} + x^{n+1} w_n (1 - xf) - 1.$$

This is equal to

$$x^{n+1}\big(-f^{n+1} + w_n(1 - xf)\big) \in x^{n+1} R[\![x]\!].$$

Since the intersection of the ideals $x^t R[\![x]\!]$ is 0, we know that $u(1 - xf) - 1 = 0$. $\square$

We can now prove that dimension goes up by 1 when adjoining a formal power series variable to a Noetherian ring.

[Hoc17, p. 129] THEOREM 8.13.2. *Let R be a Noetherian ring and let $x_1, x_2, \dots, x_k$ be indeterminates. Then,*

$$\dim\big(R[\![x_1, x_2, \dots, x_k]\!]\big) = \dim(R) + k.$$

Proof. By induction, it suffices to consider the case when $k = 1$, in which case we write $x_1 = x$. If $P \subseteq R$ is prime, then $P \cdot R[\![x]\!]$ is prime with quotient $(R/P)[\![x]\!]$ and $(P, x) \cdot R[\![x]\!]$ is prime with quotient R/P. If $P_0 \subseteq \cdots \subseteq P_n$ is a chain of prime ideals in R of length n, then their expansions

$$P_0 \cdot R[\![x]\!] \subseteq \cdots \subseteq P_n \cdot R[\![x]\!] \subseteq (P_n, x) \cdot R[\![x]\!] \tag{8.13.3}$$

is a chain of length $n+1$. We therefore see that

$$\dim\big(R[\![x]\!]\big) \geq \dim(R) + 1.$$

We now prove the converse. If R is infinite-dimensional, then $R[\![x]\!]$ is also infinite-dimensional by taking the supremum of lengths of chains of ideals as in (8.13.3). Now let Q be a maximal ideal in $R[\![x]\!]$. By Lemma 8.13.1, we know that $x \in Q$. Since Q corresponds to a maximal ideal $\mathfrak{m}$ in R under the quotient map $R[\![x]\!] \twoheadrightarrow R$, we know that $Q = (\mathfrak{m}, x) \cdot R[\![x]\!]$. If $\mathfrak{m}$ is minimal over $(r_1, r_2, \ldots, r_n)$, then Q is minimal over $(r_1, r_2, \ldots, r_n, x)$. This shows that

$$\operatorname{ht}(Q) \leq n + 1 = \operatorname{ht}(\mathfrak{m}) + 1$$

by Krull's height Theorem 8.12.2. Taking the supremum over all Q, we therefore see that

$$\dim\big(R[\![x]\!]\big) \leq \dim(R) + 1. \qquad \square$$

8.14. Dimension for modules

We now turn to dimension for modules. 11/8

Definition 8.14.1. Let M be a module over a Noetherian ring R. Let $I = \operatorname{Ann}_R(M)$. The *dimension of M* is [Hoc17, p. 138] [Hoc16b, pp. 46–48]

$$\dim(M) \coloneqq \dim(R/I).$$

If M is finitely generated, this is the same as

$$\begin{aligned}
&\sup\big\{\dim(R/P) \,\big|\, P \in \operatorname{Supp}_R(M)\big\} \\
&\quad = \sup\big\{\dim(R/P) \,\big|\, P \text{ is a minimal prime of } I\big\} \\
&\quad = \sup\big\{\dim(R/P) \,\big|\, P \in \operatorname{Ass}_R(M)\big\}
\end{aligned}$$

by Homework 10, Problem 2(a) and Corollary 8.8.3.

Proposition 8.14.2. *Let R be a Noetherian ring. If* [Hoc17, p. 138] [Hoc16b, pp. 47–48]

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is a short exact sequence of Noetherian R-modules, then

$$\dim(M) = \sup\big\{\dim(M'), \dim(M'')\big\}.$$

Moreover, if

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

is a finite filtration of M, then

$$\dim(M) = \sup\big\{\dim(M_{i+1}/M_i) \,\big|\, 0 \leq i \leq n-1\big\}.$$

Proof. By induction on n, the second statement follows from the first.

Let I', I, I'' be the annihilators of M', M, M'', respectively. Then, $I \subseteq I'$ and $I \subseteq I''$, and hence $I \subseteq I' \cap I''$. If $u \in M$, then $I''u \subseteq M'$ since I' kills $M/M' = M''$. Thus, I' kills $I''u$, i.e., $I'I''u = 0$, and hence $I'I'' \subseteq I$. Chaining these inclusions together, we have

$$(I' \cap I'')^2 \subseteq I'I'' \subseteq I \subseteq I' \cap I''.$$

Taking radicals, we obtain $\sqrt{I} = \sqrt{I' \cap I''}$, and hence $V(I) = V(I') \cup V(I'')$. $\square$

Lemma 8.14.3. *Suppose $(R, \mathfrak{m})$ is a Noetherian local ring with $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ and $M \neq 0$ is finitely generated over R. Let $I = \operatorname{Ann}_R(M)$. The following are equivalent:* [Hoc17, p. 138]

(*i*) $\ell_R\big(M/(x_1, x_2, \ldots, x_n)M\big) < \infty$.
(*ii*) $M/(x_1, x_2, \ldots, x_n)M \cong R/(x_1, x_2, \ldots, x_n) \otimes_R M$ *is supported precisely at* $\mathfrak{m}$.
(*iii*) $\operatorname{Supp}_R\big(R/(x_1, x_2, \ldots, x_n)\big) \cap \operatorname{Supp}_R(M) = \{\mathfrak{m}\}$.
(*iv*) $V(x_1, x_2, \ldots, x_n) \cap V(I) = \{\mathfrak{m}\}$.
(*v*) $\sqrt{(x_1, x_2, \ldots, x_n) + I} = \mathfrak{m}$.
(*vi*) $(x_1, x_2, \ldots, x_n)(R/I)$ *is* $(\mathfrak{m}/I)$*-primary.*

As a consequence, the least integer n *such that* $M/(x_1, x_2, \ldots, x_n)$ *is of finite length for some* $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ *is equal to* $\dim(R/I) = \dim(M)$.

Proof. These equivalences hold by the support problems on Homework 10. □

As a consequence, we can define systems of parameters for modules.

[Hoc17, p. 138] Definition 8.14.4. Let M be a finitely generated module over a Noetherian local ring $(R, \mathfrak{m})$ of dimension n. A sequence of elements $x_1, x_2, \ldots, x_n \in \mathfrak{m}$ is a *system of parameters* for M if

$$\ell_R\big(M/(x_1, x_2, \ldots, x_n)M\big)$$

is finite. By Lemma 8.14.3, $x_1, x_2, \ldots, x_n \in R$ form a system of parameters for M if and only if their images in R/I form a system of parameters for R/I. Thus, systems of parameters always exista by Corollary 8.12.5.

8.15. Regular sequences and depth

For certain modules over local rings, it is possible to construct systems of parameters that satisfy stronger properties. We define these "special" systems of parameters more generally for arbitrary modules over arbitrary rings. Rings/modules on which every system of parameters is a regular sequence form a special class of rings/modules, called *Cohen–Macaulay* rings/modules.

[Hoc16b, pp. 52–53] Definition 8.15.1. Let R be a ring and let M be an R-module. A sequence of elements $f_1, f_2, \ldots, f_k \in R$ is an *improper regular sequence* on M if

(1) f_1 is not a zerodivisor on M, i.e.,

$$M \xrightarrow{f_1 \cdot -} M$$

is injective.
(2) For all $i \in \{1, 2, \ldots, k-1\}$, f_{i+1} is not a zerodivisor on $M/(f_1, f_2, \ldots, f_i)M$, i.e.,

$$\frac{M}{(f_1, f_2, \ldots, f_i)M} \xrightarrow{f_{i+1} \cdot -} \frac{M}{(f_1, f_2, \ldots, f_i)M}$$

is injective.

and is called a *regular sequence* if moreover,

(3) $(f_1, f_2, \ldots, f_k)M \neq M$.

Note that the empty sequence is a regular sequence on any nonzero module M. Condition (3) is assumed to rule out certain degenerate situations. Otherwise, for example, the sequence $1, 1, \ldots, 1$ would be a regular sequence on 0.

Regular sequences are not necessarily permutable.

[Hoc16b, p. 53]

EXAMPLE 8.15.2. The sequence $x, (1-x)y, (1-x)z$ is a regular sequence on $R = k[x,y,z]$, while $(1-x)y, (1-x)z, x$ is not. The first sequence is a regular sequence because modulo xR, the latter two elements are $y, z \in k[y,z]$. The second sequence is not a regular sequence because

$$\frac{k[x,y,z]}{(1-x)y} \xrightarrow{(1-x)z\cdot -} \frac{k[x,y,z]}{(1-x)y}$$

maps $\bar{y}$ to $\overline{(1-x)yz} = 0$.

However, we *can* permute regular sequences in the local or graded case.

PROPOSITION 8.15.3 (Permutability of regular sequences). *Let R be a ring, let M be an R-module, and let $f_1, f_2, \ldots, f_k$ be a regular sequence on M. Suppose that one of the following conditions holds.* [Hoc16b, p. 54]

(a) *$(R, \mathfrak{m})$ is local, $f_1, f_2, \ldots, f_k \in \mathfrak{m}$, and M is finitely generated.*
(b) *R is $\mathbf{N}$-graded, M is $\mathbf{Z}$-graded with $M_{-d} = 0$ for sufficiently large d, and $f_1, f_2, \ldots, f_k$ are homogeneous of positive degree.*

For every permutation π of $1, 2, \ldots, k$,

$$f_{\pi(1)}, f_{\pi(2)}, \ldots, f_{\pi(k)}$$

is a regular sequence on M.

Proof. The permutations on $\{1, 2, \ldots, k\}$ are generated by transpositions $(i\ i+1)$ of consecutive integers. It therefore suffices to consider the case when π is such a transposition. We may replace M by $M/(f_1, f_2, \ldots, f_{i-1})M$ and hence we may assume that we are transposing f_1 and f_2. It then suffices to show that f_2, f_1 is a regular sequence, since the rest of the sequence is still a regular sequence on $M/(f_1, f_2)M = M/(f_2, f_1)M$.

We first show that f_2 is not a zerodivisor on M. Let

$$N = (0 :_M f_2) \coloneqq \{u \in M \mid f_2 u = 0\} \subseteq M.$$

(In the graded case, N is graded.) Our goal is to show that $N = f_1 N$. If $u \in N$, then $\overline{f_2 u} = 0$ in $M/f_1 M$. Since f_2 is a nonzerodivisor on $M/f_1 M$, we have $\bar{u} = 0$ in $M/f_1 M$, and hence $u = f_1 w$ for some $w \in M$. We then have

$$0 = f_2 u = f_2 f_1 w = f_1 \cdot f_2 w.$$

Since f_1 is a nonzerodivisor on M, we see that $f_2 w = 0$, which shows that $w \in N$. Thus, $N = f_1 N$, and NAK implies that $N = 0$.

It remains to show that f_1 is not a zerodivisor on $M/f_2 M$. Suppose that $f_1 \cdot \bar{v} = 0$ for $\bar{v} \in M/f_2 M$, in which case $f_1 v = f_2 u$ for some $u \in M$. Since f_2 is not a zerodivisor on $M/f_1 M$, we have that $u \in f_1 M$. We may therefore write $u = f_1 w$ for some $w \in M$. Then, $f_1 v = f_2 f_1 w$ and hence

$$f_1(v - f_2 w) = 0$$

in M. Since f_1 is not a zerodivisor on M, we see that $v = f_2 w$. □

We want a measure for how long regular sequences can be on a module. This gives another measure for the size of a module, and we will show it is bounded by above by the dimension in the local case.

DEFINITION 8.15.4. Let R be a ring and let M be an R-module. Let $I \subseteq R$ be a proper ideal. The *depth* of M on I is [Hoc16b, p. 74]

$$\operatorname{depth}_I(M) \coloneqq \sup\left\{k \geq 0 \;\middle|\; \begin{array}{c}\text{there exists a regular sequence} \\ f_1, f_2, \ldots, f_k \in I\end{array}\right\}$$

if $IM \neq M$. If $IM = M$, we set $\operatorname{depth}_I(M) = +\infty$.

REMARK 8.15.5. The convention $\operatorname{depth}_I(M) = +\infty$ is chosen so that (for example) Proposition 8.18.1 holds below.

We connect regular sequences to systems of parameters.

[Hoc20b, p. 26] PROPOSITION 8.15.6. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. Every regular sequence on M is part of a system of parameters for M. Thus,* $\operatorname{depth}_{\mathfrak{m}}(M) \leq \dim(M)$.

Proof. Taking quotients by one element of the regular sequence at a time, it suffices to show that if $f \in R$ is a nonzerodivisor on M, then

$$\dim\left(\frac{R}{I + (f)}\right) < \dim\left(\frac{R}{I}\right).$$

Since $f \in R$ is a nonzerodivisor on M, we know that $f \notin P$ for all $P \in \operatorname{Ass}_R(M)$ by Theorem 8.9.1(i). By Corollary 8.8.3, this shows that $f \notin Q$ for every Q minimal over $\operatorname{Ann}_R(M)$. □

We will later show that the maximal length of a regular sequence is always equal to the depth.

8.16. Cohen–Macaulay rings and modules

11/11

Our next goal is to show the following:

[Hoc16a, p. 14] THEOREM 8.16.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let M be a finitely generated R-module. The following conditions are equivalent.*

(i) *Every system of parameters*

$$f_1, f_2, \ldots, f_k \in \mathfrak{m}$$

for M is a regular sequence on M.

(ii) *Some system of parameters*

$$f_1, f_2, \ldots, f_k \in \mathfrak{m}$$

for M is a regular sequence on M.

In this case, for every prime ideal $P \in \operatorname{Supp}_R(M)$ such that

$$\operatorname{ht}\big(P(R/I)\big) = k$$

for $I = \operatorname{Ann}_R(M)$, there is a regular sequence of length k in P. Moreover, for every prime ideal $P \in \operatorname{Supp}_R(M)$, M_P also has the property that every system of parameters is a regular sequence.

To prove this, we start with the following:

[Hoc16b, p. 58]

Discussion 8.16.2 (Moving from one system of parameters to another). Let $(R, \mathfrak{m})$ be a Noetherian local ring of Krull dimension n and let M be a finitely generated R-module. Consider two systems of parameters

$$f_1, f_2, \ldots, f_n \qquad \text{and} \qquad g_1, g_2, \ldots, g_n$$

for M.

We claim there is a finite sequence of systems of parameters starting with $f_1, f_2, \ldots, f_n$ and ending with $g_1, g_2, \ldots, g_n$ such that any two consecutive elements of the sequence agree in all but one element. We proceed by induction on n. If $n = 1$, there is nothing to prove. Now if $n > 1$, choose $h \in \mathfrak{m}$ avoiding all

$$P \in \operatorname{Min}_R\left(\operatorname{Ann}_R\left(\frac{M}{(f_2, \ldots, f_n)M}\right)\right) \cup \operatorname{Min}_R\left(\operatorname{Ann}_R\left(\frac{M}{(g_2, \ldots, g_n)M}\right)\right).$$

Working in R/hR and lifting back to R, by the inductive hypothesis there is a finite sequence of systems of parameters connecting $h, f_2, \ldots, f_n$ and $h, g_2, \ldots, g_n$. These two systems of parameters are connected to $f_1, f_2, \ldots, f_n$ and to $g_1, g_2, \ldots, g_n$, respectively.

We can now prove Theorem 8.16.1.

Proof of Theorem 8.16.1. For the equivalence, since systems of parameters always exist (Corollary 8.12.5 and Definition 8.14.4), it suffices to show that (*ii*) $\Rightarrow$ (*i*). As in Discussion 8.16.2, we can choose a sequence of systems of parameters connecting the regular sequence $f_1, f_2, \ldots, f_n$ to a given system of parameters $g_1, g_2, \ldots, g_n$. Thus, we can reduce to the case when two systems of parameters only differ by one element. Since systems of parameters are always permutable and regular sequences are permutable in the local case (Proposition 8.15.3), we may assume that the two systems of parameters agree except possibly for the last element. We may therefore kill the first $n-1$ elements and reduce to the case where f, g are one element systems of parameters for M, where f is a nonzerodivisor on M. Letting $I = \operatorname{Ann}_R(M)$, we see that

$$\sqrt{f \cdot (R/I)} = \sqrt{g \cdot (R/I)}$$

by Lemma 8.14.3. Thus,

$$f^n \equiv rg \mod I$$

for some $r \in R$. Since f is a nonzerodivisor on M, we see that rg is also a nonzerodivisor on M. Thus, g is a nonzerodivisor on M.

For the remaining statements, let $J \supseteq I$ be an arbitrary ideal with

$$\operatorname{ht}\big(J(R/I)\big) = h$$

(i.e., the minimum height of all minimal primes of J is h). Choose a maximal (possibly empty) sequence of elements $x_1, x_2, \ldots, x_k \in J$ that is part of a system of parameters for M. If $k < h$, then $J \cdot (R/I)$ cannot be contained in the union of the minimal primes of $\operatorname{Ann}_R(M/(x_1, x_2, \ldots, x_k)M)$, for otherwise, $J \cdot (R/I)$ would be contained in one of them $Q \subseteq R/I$ by prime avoidance, while $\operatorname{ht}(Q) \leq k$. So, we can choose $x_{k+1} \in J$ not in any minimal prime of $\operatorname{Ann}_R(M/(x_1, x_2, \ldots, x_k)M)$. Then, $x_1, x_2, \ldots, x_k, x_{k+1}$ is part of a system of parameters for M, contradicting the maximality of the sequence $x_1, x_2, \ldots, x_k$.

Finally, we consider the case when $J = P$ is prime. Then, P contains a regular sequence $x_1, x_2, \ldots, x_k$ for M, which must also be regular on M_P. Since

$x_1/1, x_2/1, \ldots, x_k/1$ are a regular sequence on M_P, they are also part of a system of parameters for M_P. Since $\dim((R/I)_P) = k$, it must be a system of parameters for M_P. □

REMARK 8.16.3. There are also graded versions of Theorem 8.16.1 and Discussion 8.16.2. See [Hoc16b, p. 58] for the case when $M = R$.

We can now define:

[Hoc16a, p. 17]

DEFINITION 8.16.4. Let R be a Noetherian ring and let M be a finitely generated R-module. If R is local, we say that M is *Cohen–Macaulay* if one (equivalently, every) system of parameters for M is a regular sequence on M. In general, we say that M is Cohen–Macaulay if all of its localizations at maximal (equivalently, prime by Theorem 8.16.1) ideals in its support are Cohen–Macaulay. If $R = M$, we say that R is *Cohen–Macaulay*.

Over local rings, one way to think of this definition is that equality holds in the inequality

$$\operatorname{depth}_{\mathfrak{m}}(M) \leq \dim(M)$$

from Proposition 8.15.6. Measuring this difference leads to:

DEFINITION 8.16.5 (Serre's condition (S_k) [EGAIV$_2$, Définition 5.7.2]). Let R be a Noetherian ring and let M be a finitely generated R-module. Let k be an integer. We say that M satisfies *Serre's condition* (S_k) at a prime ideal $P \subseteq R$ if

$$\operatorname{depth}_{QR_Q}(M_Q) \geq \min\{k, \dim(M_Q)\} \tag{8.16.6}$$

for every prime ideal $Q \subseteq P$.

REMARK 8.16.7. There are differing conventions for what the condition (S_k) means when $\dim(M) < \dim(R)$. See [Vas68, Definition 1.1] for a different convention (originating from work of **S**amuel [Sam64, Proposition 6]), which replaces $\dim(M_Q)$ on the right-hand side of (8.16.6) with $\dim(R_Q)$.

[Hoc16a, p. 17]

EXAMPLES 8.16.8.

(*i*) Any regular local ring is Cohen–Macaulay since a regular system of parameters is a system of parameters and is also a regular sequence.

(*ii*) The rings

$$R = \left(\frac{k[x,y]}{(x^2,xy)}\right)_{(x,y)}$$
$$S = k[x^4, x^3y, xy^3, y^4]_{(x^4,x^3,xy^3,y^4)}$$

are not Cohen–Macaulay. In the first case, y is a system of parameters but y is a zerodivisor. In the second case, x^4, y^4 is a system of parameters but

$$y^4 \cdot (x^3y)^2 = x^4 \cdot (xy^3)^2 \in (x^4)S.$$

The ring S is known as *Macaulay's curve* [Mac94, p. 98].

(*iii*) (Gunning asked Hartshorne whether this ring is a complete intersection [Har62, Example 3.4.1]) Let k be a field and consider the coordinate ring

of the union of two coordinate planes in k^4:

$$R = \left(\frac{k[x_1,x_2,x_3,x_4]}{(x_1,x_2)\cap(x_3,x_4)}\right)_{(x_1,x_2,x_3,x_4)}$$
$$= \left(\frac{k[x_1,x_2,x_3,x_4]}{(x_1x_3,x_1x_4,x_2x_3,x_2x_4)}\right)_{(x_1,x_2,x_3,x_4)}.$$

See Figure 5.1 for an illustration. (This is also the homogeneous coordinate ring of two skew lines in $\mathbf{P}^3_k$.) The quotients $R/(x_1,x_2) \cong k[x_3,x_4]$ and $R/(x_3,x_4) \cong k[x_1,x_2]$ have dimension 2. The sequence $x_1 - x_3, x_2 - x_4$ is a system of parameters since the resulting quotient

$$\frac{R}{(x_1-x_3,x_2-x_4)} \cong \left(\frac{k[x_1,x_2]}{(x_1^2,x_1x_2,x_2^2)}\right)_{(x_1,x_2,x_3,x_4)}$$

is 0-dimensional. However, R is not Cohen–Macaulay, since

$$\frac{R}{(x_1-x_3)} \cong \left(\frac{k[x_1,x_2,x_4]}{(x_1^2,x_1x_2,x_1x_4,x_2x_4)}\right)_{(x_1,x_2,x_3,x_4)}$$

and

$$(x_2-x_4)x_1 \equiv x_1x_2 - x_1x_4 \equiv 0 \mod (x_1-x_3).$$

(*iv*) There are many more interesting examples of Cohen–Macaulay rings! Hochster even said that "Life is really worth living in a Noetherian ring R when all the local rings have the property that every s.o.p. is an R-sequence" [Hoc78, p. 887]. For example:
(1) Varieties defined by the vanishing of minors in a matrix of indeterminates [HE71].
(2) Normal monomial algebras [Hoc72b].
(3) Homogeneous coordinate rings of Grassmannians and Schubert varieties [Hoc73b; Lak72; Mus72].
(4) Invariant rings by actions of linearly reductive groups on polynomial rings [HR74].
However, there are examples for which we do not know whether they are Cohen–Macaulay. For example:
(5) Let X and Y be $n \times n$ matrices of indeterminates x_{ij} and y_{ij} over a field k. The ring

$$\frac{k[\{x_{ij}\},\{y_{ij}\}]}{(\text{entries of } XY - YX)}$$

from Conjecture 1.4.8 is conjectured to be a Cohen–Macaulay domain. This is known in dimensions $n \le 3$ [Tho86].

8.17. More on depth

One drawback to the definition of depth we have so far is that you could worry that there can be two maximal regular sequences (i.e., regular sequences that cannot be made longer) of different lengths. To prove this cannot happen, we first prove the following:

LEMMA 8.17.1. *Let R be a ring and let $x_1, x_2, \ldots, x_n$ be a regular sequence on an R-module M. Suppose that x_2 is not a zerodivisor on M. Then,* [Hoc16b, p. 74]

$$x_2, x_1, x_3, x_4, \ldots, x_{n-1}, x_n$$

is a regular sequence on M.

Proof. It suffices to show that x_1 is a nonzerodivisor on M/x_2M: since

$$\frac{M}{(x_1, x_2)M} = \frac{M}{(x_2, x_1)M},$$

the remaining conditions are unaffected by interchanging x_1 and x_2.

Suppose that $x_1u \in x_2M$, say $x_1u = x_2v$ for $v \in M$. Since x_1, x_2 is a regular sequence on M and

$$x_2v \equiv 0 \mod x_1M,$$

we have $v \in x_1M$, say $v = x_1w$. Then, $x_1u = x_2x_1w$, and $x_1(u - x_2w) = 0$. Since x_1 is a nonzerodivisor on M, we see that $u \in x_2M$ as required. □

We now show that the length of a maximal regular sequence is unique.

THEOREM 8.17.2. *Let $\theta\colon R \to S$ be a map of Noetherian rings, let M be a finitely generated S-modules, and let $I \subseteq R$ be an ideal of R. Assume that $IM \neq M$.* [Hoc16b, p. 75]

(*a*) *There is no infinite regular sequence $x_1, x_2, \ldots$ on M consisting of elements of I.*

(*b*) *There are no nonzerodivisors on M in I if and only if I is contained in the contraction of a prime in $\operatorname{Ass}_S(M)$ to R. Thus, there are no nonzerodivisors on M in I if and only if there is an element $u \in M - \{0\}$ such that $Iu = 0$.*

(*c*) *Every regular sequence in I on M (including the empty regular sequence) can be extended to a maximal regular sequence in I on M, and this maximal regular sequence is always finite.*

(*d*) *All maximal regular sequences in I on M have the same length. As a consequence, still assuming $IM \neq M$, we can define $\operatorname{depth}_I(M)$ to be the length of any maximal regular sequence on M consisting of elements in I.*

Proof. (*a*). Suppose we have an infinite regular sequence. For each $n \geq 0$, set

$$I_n = (x_1, x_2, \ldots, x_n)R.$$

Since R is Noetherian, eventually we have $I_n = I_{n+1}$. This means that $x_{n+1} \in I_n$, and hence x_{n+1} kills M/I_nM. Since x_{n+1} is not a zerodivisor on M/I_nM, we must have $M/I_nM = 0$, and hence $M = I_nM$. Since $I_n \subseteq I$, we see that $M = IM$, a contradiction.

(*b*). Fix an element $x \in R$. Write

$$\operatorname{Ass}_S(M) = \{Q_1, Q_2, \ldots, Q_n\}.$$

Then, x is a zerodivisor on M (considered as an R-module) if and only if $\theta(x)$ is a zerodivisor on M (considered as an S-module). By Theorem 8.9.1(*i*), this holds if and only if $\theta(x) \in Q_i$ for some i. Ranging over all $x \in I$, we see that I consists entirely of zerodivisors on R if and only if

$$I \subseteq \bigcup_i (Q_i \cap R),$$

where we recall that the notation $Q_i \cap R$ is used for $\theta^{-1}(Q_i)$ even if θ is not injective. By prime avoidance, we see that $I \subseteq Q_i \cap R$ for some i.

For the last statement, we know there exists $u \in M - \{0\}$ such that $\mathrm{Ann}_S(u) = Q_i$. Then, since $\theta(I) \subseteq Q_i$, we see that $Iu = 0$.

(c). Suppose we have a regular sequence $x_1, x_2, \ldots, x_k$ and let

$$I_k = (x_1, x_2, \ldots, x_k)R.$$

If every element of I is a zerodivisor on M/I_kM, then we have constructed the required maximal regular sequence on M in I. If not, we can enlarge the regular sequence by taking an element $x_{k+1} \in I$ avoiding all associated primes of M/I_kM. We can continue recursively in this way. The process must terminate by (a).

(d). Suppose we have a counterexample. Since M is Noetherian, there is a maximal $N \subseteq M$ such that M/N provides a counterexample. Replacing M by M/N, we may therefore assume that (d) holds for every proper homomorphic image of M. If every element of I is a zerodivisor on M, then the empty sequence is the unique maximal regular sequence on M. 11/13

Now suppose

$$x_1, x_2, \ldots, x_h \qquad \text{and} \qquad y_1, y_2, \ldots, y_k$$

are two maximal regular sequences on M consisting of elements in I. After switching the two sequences, we may assume that $h \leq k$. We induce on h. The case $h = 0$ was shown in the previous paragraph.

Suppose $h = 1$. We denote $x \coloneqq x_1$ and $y \coloneqq y_1$. Then, I consists entirely of zerodivisors on M/xM. By (b), there exists an element $u \in M - xM$ such that $Iu \subseteq xM$. We want to show that y is also a maximal regular sequence. Since $Iu \subseteq xM$, we can write

$$yu = xv$$

for some $v \in M$. We have $v \notin yM$ since if $v = yw$, then $yu = xyw$ and the fact y is a nonzerodivisor implies $u = xw \in xM$, which contradicts the choice $u \in M - xM$. To finish this case, by (b), it suffices to show that $Iv \subseteq yM$. Let $f \in I$. Then, we have

$$xfv = f(xv) = f(yu) = y(fu) = y(xw)$$

for some $w \in M$ since $Iu \subseteq xM$. But then, $x(fv - yw) = 0$, and since x is a nonzerodivisor on M, we conclude that

$$fv = yw \in yM$$

as required.

Finally, suppose that $h \geq 2$. Then, the contractions to R of associated primes in $\mathrm{Ass}_S(M/x_1M)$ do not cover I (they miss x_2). Similarly, the contractions to R of associated primes in $\mathrm{Ass}_S(M/y_1M)$ do not cover I (they miss y_2). Likewise, the contractions to R of associated primes in $\mathrm{Ass}_S(M)$ do not cover I (they miss x_1, y_1). Thus, by prime avoidance, the union of the primes in the union of all three sets does not cover I. We can therefore find $z \in I$ that is not in any of them. Then, by (c), x_1, z and y_1, z are regular sequences on M and can be extended to a maximal regular sequence on M in I, say

$$x_1, z, x_3', \ldots, x_{h'}' \qquad \text{and} \qquad y_1, z, y_3', \ldots, y_{k'}'.$$

Working in M/x_1M, we know that $h = h'$ by the inductive hypothesis. Working in M/y_1M, we know that $k = k'$ by the inductive hypothesis. Since z is a nonzerodivisor on M, the sequences

$$z, x_1, x_3', \dots, x_{h'}' \qquad \text{and} \qquad z, y_1, y_3', \dots, y_{k'}'$$

are also regular sequences by Lemma 8.17.1. Working in M/zM, we know that $h' = k'$ by the inductive hypothesis. Thus, we see that $h = h' = k' = k$. □

8.18. Depth in short exact sequences

We now show that depth, like, dimension, behaves well in short exact sequences. This result (and many of the previous results) is usually proved using a characterization of depth using Ext modules. See, for example, [BH98, Proposition 1.2.9]. According to Hochster, these proofs are "very slick, but in some ways mask the simplicity of what is going on" [Hoc16b, p. 74].

PROPOSITION 8.18.1. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Consider a short exact sequence*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of finitely generated R-modules for which the depth on I is finite.

(*i*) $\operatorname{depth}_I(M) \geq \min\{\operatorname{depth}_I(M'), \operatorname{depth}_I(M'')\}$.
(*ii*) *If* $\operatorname{depth}_I(M) > \operatorname{depth}_I(M'')$, *then* $\operatorname{depth}_I(M') = \operatorname{depth}_I(M'') + 1$.

Proof. We identify M' with its image in M to assume that $M' \subseteq M$.

(*i*). We induce on

$$d \coloneqq \min\big\{\operatorname{depth}_I(M'), \operatorname{depth}_I(M'')\big\}.$$

If $d = 0$, then there is nothing to show. It therefore suffices to consider the case when $d > 0$, in which case

$$\operatorname{depth}_I(M') > 0 \qquad \text{and} \qquad \operatorname{depth}_I(M'') > 0,$$

and therefore I is not contained in the union of primes in $\operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'')$. Choose $x \in I$ that avoids all these associated primes, in which case x avoids the associated primes of M as well by Proposition 8.6.3(*ii*). Then, x is a nonzerodivisor on all three modules by Theorem 8.9.1(*i*). We therefore have the commutative diagram

(8.18.2)

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & xM' & \longrightarrow & xM & \longrightarrow & xM'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'/xM' & \longrightarrow & M/xM & \longrightarrow & M''/xM'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the first row is isomorphic to the second row by the fact that x is a nonzerodivisor on all three modules. We now have

$$\begin{aligned}\operatorname{depth}_I(M/xM) &\geq \min\bigl\{\operatorname{depth}_I(M'/xM'), \operatorname{depth}_I(M''/xM'')\bigr\}\\ &= \min\bigl\{\operatorname{depth}_I(M'), \operatorname{depth}_I(M'')\bigr\} - 1\end{aligned}$$

by the inductive hypothesis, and hence $\operatorname{depth}_I(M) \geq d$ by Theorem 8.17.2(*d*).

(*ii*). We induce on $\operatorname{depth}_I(M'')$. If $\operatorname{depth}_I(M'') = 0$, choose $u \in M - \{0\}$ such that I kills the image of u in M''. Choose any nonzerodivisor $f \in I$ on M. Then, f is a nonzerodivisor on $M' \subseteq M$, and $fu \in M'$, since I kills the image of u in M''. We want to show that f is a maximal regular sequence on M'. We have $fu \notin fM'$, for otherwise $u \in M'$ in which case the image of u in M'' would equal 0. However,

$$I(fu) = f(Iu) \subseteq fM',$$

and hence the image of fu in M'/fM' is a nonzero element killed by I. By Theorem 8.17.2(*b*), this shows that f is a maximal regular sequence on M consisting of elements in I.

It remains to prove the case when $\operatorname{depth}_I(M'') > 0$. If $\operatorname{depth}_I(M'') > 0$, then all three depths are positive. We can now choose $x \in I$ that avoids the associated primes of M'', M, M'. Using the diagram (8.18.2) again, we see that

$$\begin{aligned}\operatorname{depth}_I(M') &= \operatorname{depth}_I(M'/xM') + 1\\ &= \operatorname{depth}_I(M''/xM'') + 2\\ &= \operatorname{depth}_I(M''/xM'') + 1\end{aligned}$$

by the inductive hypothesis. □

This concludes what I wanted to tell you about Cohen–Macaulayness. You will see more if you take Commutative Algebra II in the spring!

CHAPTER 9

Normal rings, DVRs, and Dedekind domains

Our next objective is to study some different characterizations of normal Noetherian domains, and apply them to the study of normal Noetherian domains of Krull dimension one.

9.1. Dedekind domains

We start by defining the class of rings we will eventually want to study.

DEFINITION 9.1.1. A *Dedekind domain* is a normal Noetherian domain of Krull dimension one.

Recall that we defined a DVR to be a local PID that is not a field. DVR's are all examples of Dedekind domains, and more generally, every PID that is not a field is a Dedekind domain. We will eventually want to show that Dedekind domains are a non-local analogue of DVR's.

EXAMPLE 9.1.2. The prototypical example of a Dedekind domain are *rings of algebraic integers*. These are formed by taking the integral closure of $\mathbf{Z}$ in a finite extension F of $\mathbf{Q}$. [Hoc17, p. 138]

You may be worried that rings of algebraic integers may not be Noetherian; this will not end up being the case.

9.2. Krull and Serre's criteria for normality

We will need to first characterize DVR's.

PROPOSITION 9.2.1. *Let R be a Noetherian ring, and suppose that P is an associated prime of $R/(x)$ for a nonzerodivisor $x \in R$. Then, P is an associated prime of $R/(y)$ for every nonzerodivisor $y \in P$.* [Hoc17, p. 139]

Proof. The conditions don't change when passing from R to R_P, and so we replace R by (R_P, PR_P) to assume that R is local with maximal ideal P. Since $P \in \mathrm{Ass}_R(R/(x))$, there exists an element $a \in R - (x)$ such that the annihilator of the image of a in $R/(x)$ is P. We therefore have $Pa \subseteq (x)$. Write $ya = xb$ for $b \in R$.

We claim that $b \notin (y)$. Otherwise, $b = yr$, in which case $ya = xyr \Rightarrow y(a - xr) = 0 \Rightarrow a = xr$ since y is a nonzerodivisor, contradicting the fact that $a \notin (x)$. We therefore see that $b \notin (y)$.

We now show that $Pb \subseteq (y)$, which proves the statement of the proposition since P is maximal. If $u \in P$, then $ua = xs$ for some $s \in R$ as before. Since $ya = xb$, we see that $uxb = uya = yxs$, and hence $x(ub - ys) = 0 \Rightarrow ub = ys$, since x is a nonzerodivisor. □

PROPOSITION 9.2.2. *A Noetherian local domain (R, P) that is not a field is a DVR if and only if $P = (y)$ is principal.* [AK21, (23.9)] [Hoc17, p. 139]

We note that by definition of a regular local ring (Definition 8.12.4), the last condition holds if and only if R is a regular local ring of dimension one.

Proof. The direction $\Rightarrow$ is clear by definition of a DVR. Conversely, suppose $P = (y)$, and consider any nonzero element $r \in P$. Since $\bigcap_n P^n = 0$ by Krull's intersection theorem Theorem 8.10.1, there is a largest integer $n \geq 1$ such that $r = uy^n$ for $u \in R$. Then, y does not divide u, and hence $u \in R - P$ is a unit. Thus, every nonzero non-unit is a unit times a power of y. It follows that any proper nonzero ideal is generated by the least power of y that it contains. □

11/15

We can now characterize Noetherian normal domains. This theorem is due to Krull [Kru32].

[AK21, (23.15)]
[Rei95, pp. 119–120]
[Hoc17, p. 139]

THEOREM 9.2.3 (Krull's criterion for normality [Kru32]). *A Noetherian domain R is normal if and only if both of the following conditions hold:*

(1) *Every associated prime of every nonzero principal ideal has height 1.*
(2) *The localization of R at every height 1 prime is a DVR.*

In particular, if R is one-dimensional and local, then R is normal if and only if R is a DVR.

Proof. We first show $\Rightarrow$. Let x be any nonzero element of R and let $P \in \mathrm{Ass}_R(R/(x))$.

CLAIM 9.2.4. *It suffices to show that R_P is a DVR for every such P.*

This would show that $\mathrm{ht}(P) = 1$. Moreover, since every height 1 prime in R is the minimal prime of some nonzero element contained in it by Krull's principal ideal theorem (Theorem 8.12.1), this will show that R_P is a DVR for every height 1 prime in R.

From now on, we replace R by R_P to assume that R is local. Since $P \neq 0$, we know that $P \neq P^2$ by NAK. Choose $y \in P - P^2$. We will prove that $(y) = P$, which would show that $\mathrm{ht}(P) = 1$ and that $R = R_P$ is a DVR by Proposition 9.2.2.

Note that P is an associated prime of $R/(y)$ by Proposition 9.2.1. Thus, there exists an element $a \in R - (y)$ such that

$$Pa \subseteq (y).$$

If a is a unit, then $P \subseteq (y)$, and since $y \in P$, equality holds and we are done.

If a is not a unit, then $a \in P$ (since R is local), and we will obtain a contradiction. First, we know that $Pa \subseteq yP$, for otherwise if we could write $ra = yu$ for $r \in P$ and u a unit, then $yu \in P^2$, and hence $y \in P^2$, a contradiction. Our goal is to show that this implies $a \in (y)$, which would be a contradiction. Let $f_1, f_2, \ldots, f_n$ be a set of generators for P. For every i, the inclusion $Pa \subseteq yP$ implies

$$af_i = y \sum_j r_{ij} f_j$$

for some elements $r_{ij} \in R$. If we make $f_1, \ldots, f_n$ into a column vector V and let A be the matrix (r_{ij}), then we have $AV = (a/y)V$ in the fraction field K of R. The entries of V generate the nonzero prime P, and is an eigenvector for A with eigenvalue a/y. By linear algebra, a/y satisfies the characteristic polynomial of the matrix $A = (r_{ij})$, which is a monic polynomial with coefficients in R. Since R is normal, this implies $a/y \in R$, and hence $a \in (y)$, a contradiction.

We now show $\Leftarrow$. We proceed by contradiction. Suppose that R is not normal and let $\alpha \in K = \mathrm{Frac}(R)$ be an element not in R that is integral over R. Then,

$M = R[\alpha]/R$ is a finitely generated nonzero R-module, and hence by Lemma 8.6.4 there is a prime ideal $P \in \mathrm{Ass}_R(M)$. Our hypotheses (1) and (2) are preserved when passing from R to R_P, and

$$PR_P \in \mathrm{Ass}_{R_P}(M_P)$$

by Proposition 8.8.1. We therefore see that $M_P \neq 0$, which means that $R_P[\alpha]$ is strictly larger than R_P, i.e., R_P is not normal.

From now on, we replace R by R_P to assume that (R, P) is local. Choose $\beta \in R[\alpha]$ such that

$$P = \mathrm{Ann}_R(\bar{\beta}), \tag{9.2.5}$$

where $\bar{\beta}$ is the image of β in $R[\alpha]/R$. Write $\beta = a/x$ where $x \in R - \{0\}$ and $a \notin xR$. Rewriting the condition (9.2.5), we have that $P(a/x) \subseteq R$ inside of $K = \mathrm{Frac}(R)$, which implies $Pa \subseteq xR$. This implies that P is contained in an associated prime of $R/(x)$. Since P is maximal, we see that P itself is an associated prime of $R/(x)$, and has height 1 by (1). But then, $R = R_P$ is not normal by the choice of P in the previous paragraph, contradicting (2). □

As a result, we have the following characterization of Dedekind domains:

Corollary 9.2.6. *A Noetherian domain R of Krull dimension one is a Dedekind domain if and only if for every maximal ideal $P \subseteq R$, the localization R_P is a DVR.* [AK21, (24.7)] [Hoc17, p. 142]

Proof. Normality is a local condition. □

We also state a generalization of Krull's criterion for normality (Theorem 9.2.3) due to Serre. Serre's criterion uses the following:

Definition 9.2.7 [EGAIV$_2$, Définition 5.8.2]. Let R be a Noetherian ring and let k be an integer. We say that R satisfies *condition* (R_k) if R_P is a regular local ring for every prime ideal $P \subseteq R$ of height $\leq k$.

Theorem 9.2.8 (Serre's criterion for normality [EGAIV$_2$, Théorème 5.8.6]). *Let R be a Noetherian ring. The following are equivalent.* [Mat89, Thm. 23.8]

- (*i*) *R is a Noetherian normal ring, i.e., R_P is a normal domain for every prime ideal $P \subseteq R$.*
- (*ii*) *R satisfies (R_1) and (S_2).*

Proof. (*i*) $\Rightarrow$ (*ii*). We first show (R_1). Letting P be a height 1 prime, we know that R_P is normal, and hence R_P is a DVR by condition (2) in Theorem 9.2.3.

To show (S_2), there are two cases. Let $Q \subseteq R$ be a prime ideal. We want to show that

$$\mathrm{depth}_{QR_Q}(R_Q) \geq \min\{2, \dim(R_Q)\}.$$

If $\dim(R_Q) \leq 1$, then R_Q is a regular local ring (either $\mathrm{ht}(Q) = 0$, in which case R_Q is a field, or $\mathrm{ht}(Q) = 1$, in which case R_Q is a DVR) and hence has depth equal to $\dim(R_Q)$. If $\dim(R_Q) \geq 2$, we need to show that $\mathrm{depth}_{QR_Q}(R_Q) \geq 2$. Choose a nonzero element $x \in R_Q$, which is a nonzerodivisor since R_Q is a domain. Since the associated primes of R_Q/xR_Q are all of height 1 by condition (1) in Theorem 9.2.3, we know that the associated primes of R_Q/xR_Q cannot cover QR_Q by prime avoidance. We can therefore find

$$y \in QR_Q - \bigcup_{P \in \mathrm{Ass}_{R_Q}(R_Q/xR_Q)} P.$$

This shows that x, y is a regular sequence on R_Q, i.e., $\operatorname{depth}_{QR_Q}(R_Q) \geq 2$.

$(ii) \Rightarrow (i)$. Let

$$(0) = Q_1 \cap Q_2 \cap \cdots \cap Q_r$$

be an irredundant primary decomposition for $(0) \subseteq R$. We claim that the Q_i are minimal primes. There cannot be any embedded primes P because otherwise, localizing at P, the resulting ring R_P has $\operatorname{depth}_{PR_P}(R_P) = 0$, and hence will not satisfy (S_2) (or even (S_1)!). Moreover, each Q_i is prime since R_{P_i} is reduced, and hence

$$(0) \cdot R_{P_i} = Q_i \cdot R_{P_i}$$

is prime and contracts to the prime ideal $Q_i \subseteq R$. We therefore see that

$$R \cong \prod_i \frac{R}{Q_i}$$

by the Chinese Remainder Theorem 4.5.5. For every prime ideal $P \subseteq R$, we know that it contains some Q_i, and hence

$$R_P \cong \left(\frac{R}{Q_i}\right)_P.$$

The ring R_P is a normal domain since it is the localization of a domain, (S_2) implies (1), and (R_1) implies (2). □

9.3. Primary decomposition and divisor class groups

We now study primary decomposition in normal domains, with the specific goal of understanding Dedekind domains. We start with the following:

Observation 9.3.1. Let R be a normal Noetherian domain. For a principal ideal $(f) \subseteq R$, the primary decomposition is particularly nice:

(1) By Krull's criterion for normality (Theorem 9.2.3), we know that there are no embedded primes, and so if $0 \neq f \in P$, the P-primary component of (f) is unique and corresponds to the contraction of an ideal primary to the maximal ideal in R_P, a DVR.
(2) Since the only ideals primary to PR_P in R_P are powers of PR_P, every P-primary ideal in the decomposition for (f) is of the form $P^{(k)}$ for some k.

Thus, if $f \neq 0$ is not a unit, we have a unique irredundant primary decomposition

$$(f) = P_1^{(k_1)} \cap P_2^{(k_2)} \cap \cdots \cap P_n^{(k_n)}. \tag{9.3.2}$$

[Hoc17, p. 140] Definition 9.3.3. Let R be a normal Noetherian domain. Consider the free Abelian group G on generators $[P]$ corresponding bijectively to height 1 prime ideals P of R. A *divisor* is an element in G. A divisor is *principal* if there exists an element $f \in R - \{0\}$ such that

$$\operatorname{div}(a) \coloneqq \sum_{i=1}^{n} k_i [P_i],$$

where the P_i and k_i are those coming from the primary decomposition for (f) as in (9.3.2). The divisor of a unit is 0 by convention. If $I \subseteq R$ is an ideal of *pure height* 1 (i.e., every prime appearing in an irredundant primary decomposition for I is of height 1), then we can similarly define the divisor $\operatorname{div}(I)$ associated to I by taking an irredundant primary decomposition for it as in (9.3.2).

The *divisor class group* of R is the quotient group

$$\mathrm{Cl}(R) \coloneqq \frac{G}{\mathbf{Z} \cdot \big\{ \mathrm{div}(f) \;\big|\; f \in R - \{0\} \big\}}.$$

We note that the divisor associated to every principal ideal vanishes in $\mathrm{Cl}(R)$. 11/18
We use this to characterize when a ring is a UFD.

THEOREM 9.3.4. *Let be a normal Noetherian domain.* [Hoc17, pp. 140–141]

(*i*) *If I is an ideal of pure height 1, then fI is also of pure height 1 for every $f \in R - \{0\}$, and we have*

$$\mathrm{div}(fI) = \mathrm{div}(f) + \mathrm{div}(I).$$

(*ii*) *Let I and J be ideals of pure height 1. Then, $\mathrm{div}(I) = \mathrm{div}(J)$ if and only if $I = J$. The images of $\mathrm{div}(I)$ and $\mathrm{div}(J)$ are equal in $\mathrm{Cl}(R)$ if and only if there are nonzero elements $f, g \in R$ such that $fI = gJ$, which holds if and only if I and J are isomorphic as R-modules.*

(*iii*) *An ideal I of pure height 1 is principal if and only if $\mathrm{div}(I)$ is 0 in $\mathrm{Cl}(R)$. Thus, R is a UFD if and only if $\mathrm{Cl}(R) = 0$.*

(*iv*) *The elements of $\mathrm{Cl}(R)$ are in bijective correspondence with isomorphism classes of pure height 1 ideals considered as R-modules, where the inverse of the element represented by $\mathrm{div}(I)$ is given by $\mathrm{div}(J)$, where J is a pure height 1 ideal such that*

$$J \cong \mathrm{Hom}_R(I, R).$$

In fact, if $g \in I - \{0\}$, then one can take $J = (gR :_R I)$.

Proof. We first show (*i*) and (*ii*). First, $I = J$ if and only if $\mathrm{div}(I) = \mathrm{div}(J)$ since for pure height 1 ideals, the associated divisor completely determines the primary decomposition of the ideal as in (9.3.2). For (*i*), we consider the short exact sequence

$$0 \longrightarrow R/I \xrightarrow{f\cdot} R/fI \longrightarrow R/fR \longrightarrow 0.$$

Injectivity on the left holds by the fact that $R \xrightarrow{f\cdot} R \to R/fI$ has kernel equal to I by the assumption that R is a domain. We obtain the inclusion

$$\mathrm{Ass}_R(R/fI) \subseteq \mathrm{Ass}_R(R/I) \cup \mathrm{Ass}_R(R/fR).$$

and hence R/fI is also of pure height 1. The equality

$$\mathrm{div}(fI) = \mathrm{div}(f) + \mathrm{div}(I)$$

can be checked after localizing at each height one prime ideal Q (this uses Proposition 8.8.5, which says that primary decompositions localize well), in which case we reduce to the DVR case, which holds since every ideal is a power of the (principal) maximal ideal.

We now prove the second statement in (*ii*). By (*i*), we know that

$$\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$$

for all $f, g \in R - \{0\}$, and hence

$$\mathbf{Z} \cdot \big\{ \mathrm{div}(f) \;\big|\; f \in R - \{0\} \big\} = \big\{ \mathrm{div}(g) - \mathrm{div}(f) \;\big|\; f, g \in R - \{0\} \big\}.$$

Thus, if the images of $\mathrm{div}(I)$ and $\mathrm{div}(J)$ are equal in $\mathrm{Cl}(R)$, then

$$\mathrm{div}(I) - \mathrm{div}(J) = \mathrm{div}(g) - \mathrm{div}(f),$$

and hence $\operatorname{div}(fI) = \operatorname{div}(gJ)$ and $fI = gJ$. For the last statement, we first note that $fI = gJ$ implies that I and J are isomorphic as R-modules since R is a domain. For the converse, suppose

$$\theta\colon I \xrightarrow{\sim} J$$

is an isomorphism of R-modules (we do not need that I and J are of pure height 1 here). By Problem 4 on Homework 8, θ is of the form $\theta(x) = (f/g)x$ for some $f/g \in \operatorname{Frac}(R)$. This yields that $(f/g)I = J$, and hence $fI = gJ$.

For (*iii*), the first statement follows by setting $J = R$ in (*ii*). For the second statement, it suffices to show that R is a UFD if and only if every height 1 prime is principal. We saw the direction $\Rightarrow$ in Lemma 5.5.3. For the converse, it suffices to show that every irreducible element $f \in R - \{0\}$ is prime. Every minimal prime P of (f) is of height 1 by Krull's Principal Ideal Theorem 8.12.1, and is therefore principal: $P = (g)$. Then, $f = ug$ for some $u \in R$, which must be a unit by the irreducibility of f. We therefore see that $(f) = P$, which shows that R is a UFD.

It remains to show the description of the inverse in (*iv*), since the first part follows from (*ii*) and the fact that inverses are also divisors of ideals. Fix a nonzero ideal I and fix an element $g \in I - \{0\}$. In Homework 8, Problem 4, you showed that

$$\operatorname{Hom}_R(I, R) = \big\{ f/g \in \operatorname{Frac}(R) \;\big|\; (f/g)I \subseteq R \big\}$$

where f is the image of g in R. An element $f \in R$ is contained in the right-hand side if and only if $fI \subseteq gR$, and hence the set on the right-hand side is equal to

$$(gR :_R I) = \big\{ f \in R \;\big|\; fI \subseteq gR \big\}.$$

We will show that setting $J = (gR :_R I)$, the ideal J has pure height 1 (even if I does not), and that if I has pure height 1, then

$$\operatorname{div}(J) + \operatorname{div}(I) = \operatorname{div}(g),$$

which would show that $\operatorname{div}(J) = -\operatorname{div}(I)$ in $\operatorname{Cl}(R)$.

Suppose R/J has an associated prime P of height at least 2. We localize at P to assume that every element not in P is a unit. The condition for P to be an associated prime of R/J is that there is an element $u \notin J$ such that that $Pu \subseteq J$. In terms of the definition of J, there exists an element $u \in R$ such that $uI \not\subseteq gR$, but such that $PuI \subseteq gR$. Choose $r \in I$ such that $ur \notin gR$. Then, $Pur \subseteq gR$, and since every element not in P is a unit, this shows that P is an associated prime of $R/(g)$, contradicting Krull's criterion for normality (Theorem 9.2.3).

We now show that if I is of pure height 1, then

$$\operatorname{div}(J) + \operatorname{div}(I) = \operatorname{div}(g).$$

It suffices to show that the coefficients of each height 1 prime P in $\operatorname{div}(I)$ and $\operatorname{div}(J)$ add up to the coefficient of P in $\operatorname{div}(g)$. It suffices to check this after localizing at P. After localization, if x generates the maximal ideal in R_P, we have $I = (x^m)$ and $(g) = (x^{m+n})$ where $m, n \in \mathbf{N}$. Since the formation of colon ideals commutes with localization (Proposition 7.13.3), we see that

$$J = \big((x^{m+n}) :_R (x^n)\big) = (x^m). \qquad \square$$

Example 9.3.5. It is hard to give explicit computations of divisor class groups, but we do know that they measure how far a normal domain is from being a UFD.

The ring $\mathbf{Z}[\sqrt{-5}]$ is not a UFD since

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Assuming it is a Dedekind domain, there is therefore a prime ideal of height 1 that is not principal. The ideal $(2, 1 + \sqrt{-5})$ is one of these.

An important consequence of our discussion for Dedekind domains is the following:

THEOREM 9.3.6 (Main theorem of classical ideal theory). *Let R be a Dedekind domain. Then, every nonzero ideal I has a unique factorization* [AK21, (24.10)] [Hoc17, p. 142]

$$I = \prod_P P^{v_P(I)},$$

into primes P, where $v_P(I)$ is the integer k_P such that $I_P = P^{k_P} R_P$.

In other words, while there is no unique factorization into products of irreducible elements, there is still unique factorization of ideals into products of prime ideals!

Proof. Every nonzero ideal in R is of pure height 1. Thus, I has an irredundant primary decomposition of the form

$$I = P_1^{(v_{P_1}(I))} \cap P_2^{(v_{P_2}(I))} \cap \cdots \cap P_n^{(v_{P_n}(I))}.$$

Now $P^{(k)} = P^k$ since symbolic powers of maximal ideals coincide with usual powers (powers of maximal ideals are already P-primary by Proposition 8.2.6(i), and use the correspondence in Proposition 8.2.6(ii)). Now the fact that we can replace intersections with products is a consequence of the Chinese Remainder Theorem 4.5.5. □

Computing the class group is difficult, even for Dedekind domains, and is one important aspect of algebraic number theory. One reason to think that computing class groups would be difficult is the following result of Claborn:

THEOREM 9.3.7 [Cla66, Theorem 7]. *Every Abelian group is the divisor class group of a Dedekind domain.*

Moreover, Leedham-Green showed that one can construct such a Dedekind domain using a geometric construction using affine plane curves [LG72], and Rosen gave a more number-theoretic construction [Ros73; Ros76].

Before we move on to the next topic, we give one example from algebraic geometry.

EXAMPLE 9.3.8. Let k be a field, and consider [Har77, Ch. II, Ex. 6.5.2]

$$R = \frac{k[x, y, z]}{(xy - z^2)}.$$

This is the coordinate ring of an affine quadric cone in k^2. If $k = \mathbf{R}$, you can visualize this as a cone in $\mathbf{R}^2$ in (almost) the usual sense.

Consider a ruling of the cone given by the line $y = z = 0$, corresponding to the prime ideal $P = (y, z)$. We claim this gives a nonzero element in $\mathrm{Cl}(R)$, such that $2 \cdot \mathrm{div}(P) = 0$. The ideal P is not principal since at the origin $\mathfrak{m} = (x, y, z)$, the vector space $\mathfrak{m}/\mathfrak{m}^2$ is three-dimensional over k, and the image of $P = (y, z)$ in

$\mathfrak{m}/\mathfrak{m}^2$ is at least two-dimensional. Now to show that $2 \cdot \operatorname{div}(P) = 0$, we claim that $2 \cdot \operatorname{div}(P) = \operatorname{div}(y)$. Since

$$\frac{R}{(y)} \cong \frac{k[x,z]}{(z^2)}$$

has only one associated prime (y,z), we see that in an irredundant primary decomposition for (y), the only prime that can show up is P. It remains to identify what symbolic power of P should be equal to (y). We claim that $P^{(2)} = (y)$. First, we note that in R_P, the maximal ideal is (y,z). But $x \notin (y,z)$, and hence $x^{-1} \in R_P$, which gives $y = x^{-1}z^2$. Thus, the maximal ideal in R_P is generated by (z). We then have

$$P^2 R_P = (z^2) = (x^{-1}z^2) = (y),$$

and hence $(y) = P^{(2)}$.

This is connected to the following:

Conjecture 9.3.9 (Eisenbud–Mazur [EM97, p. 190]). *Let*

$$P \subseteq \mathbf{C}[\![x_1, x_2, \dots, x_n]\!]$$

be a prime ideal, and set $\mathfrak{m} = (x_1, x_2, \dots, x_n)$. *Is it true that* $P^{(2)} \subseteq \mathfrak{m}P$*?*

In other words, the peculiarities in the example above should not occur for regular local rings containing the complex numbers (or any other field of characteristic zero).

Remark 9.3.10. The Eisenbud–Mazur Conjecture 9.3.9 is sometimes *false* for regular local rings of positive characteristic [EM97, p. 190] and for regular local rings not containing a field [KR00, Remark 3.3(b)].

9.4. More on normal domains

11/20

We will prove a few more results about normal domains before discussing the classification of modules over a Dedekind domain. We start with the following result, which Vakil calls the *algebraic Hartogs's lemma* [Vak, (13.5.1)].

[AK21, (23.18)]
[Rei95, p. 121]
[Hoc17, p. 143]

Theorem 9.4.1 (Algebraic Hartogs's lemma). *A Noetherian domain R is normal if and only if it is the intersection of DVRs in the fraction field K of R. In this case, the DVRs may be taken to be its localizations at height 1 primes, i.e.,*

$$R = \bigcap_{\operatorname{ht}(P)=1} R_P.$$

Proof. As a DVR is normal, an intersection of DVRs is normal, showing $\Leftarrow$. Thus, it suffices to show that a normal Noetherian domain is the intersection of its localizations at height 1 primes. Since R is a domain, R is contained in this intersection, and hence it suffices to show the converse. Let $f = a/x \in \operatorname{Frac}(R)$ be a fraction in this intersection and suppose it does not lie in R. Consider the module

$$M = \frac{R + R(a/x)}{R}$$

which is nonzero. Then, a/x has some nonzero multiple b/x with prime annihilator P modulo R. We replace R by R_P. Then, $b/x \notin R$ but $P(b/x) \subseteq R$, which says that $b \notin xR$ but $Pb \subseteq xR$. This implies that $P \in \operatorname{Ass}_R(R/(x))$ because $P = \operatorname{Ann}_R(\bar{b})$, where $\bar{b}$ is the image of b in $R/(x)$. Since R is normal, we see that P is a height

1 prime and R is a DVR. But then, $b/x \in R$ since b/x was chosen to be in the localization of R at all height 1 primes, a contradiction. □

We also show:

THEOREM 9.4.2. *A polynomial ring (even in infinitely many variables) over a normal Noetherian domain is normal.* [Hoc17, p. 143]

Proof. A union of normal domains is normal, since an element α in the fraction field integral over the union will be in the fraction field of one of these domains, and will be integral over one of them. But then, some domain D in the family contains both of these, and since D is normal, α is integral over D and is in the fraction field of D, and so must be in D.

It therefore suffices to consider the case of finitely many variables. By induction, we can also reduce to the case of one variable. Since the ring R is the intersection of DVRs $V \subseteq \mathrm{Frac}(R)$, it follows that $R[x]$ is the intersection of rings $V[x] \subseteq \mathrm{Frac}(R)[x]$. Since every $V[x]$ is a UFD, it is normal. Thus, $R[x]$ is normal. □

REMARK 9.4.3. The same proof works for formal power series in finitely many variables, provided one shows that $V[\![x]\!]$ is a UFD. One proof of this uses the theory of regular local rings. For non-Noetherian rings, the polynomial case is still true, but the formal power series case is false in general. [Hoc17, p. 143]

9.5. Noetherianity of integral closures

We now come to an important missing piece of the puzzle in our discussion of Dedekind domains.

QUESTION 9.5.1. *Let R be a Noetherian domain and let $K = \mathrm{Frac}(R)$. Is the normalization of R in K or a finite field extension $K \subseteq L$ still Noetherian?*

The answer is no in general, but here are some cases when it is true:

(1) When R is normal and $K \subseteq L$ is separable. Since separability is automatic when $\mathrm{char}(k) = 0$, this implies that rings of algebraic integers are Noetherian.
(2) When R is finitely generated as an algebra over a field.

In these cases, the integral closure of R is in fact *module-finite*. This leads to the following:

DEFINITION 9.5.2 [Mat80, (31.A)]. A domain R with fraction field K is *N-1* if the integral closure of R in K is module-finite, and is *N-2* if the integral closure of R in L is module-finite for every finite field field extension $K \subseteq L$.

The terminology in [EGAIV$_1$, **0**, Définition 23.1] is *Japanese*. There are Noetherian domains that are not N-1, so you should think of Noetherian N-1 domains as a particular subclass of rings that gets rid of pathologies. In practice, most Noetherian domains one encounters in number theory and algebraic geometry are in fact N-1.

THEOREM 9.5.3. *Let R be a normal Noetherian domain and let L be a finite separable extension of $K = \mathrm{Frac}(R)$. Then, the integral closure S of R in L is module-finite over R, and hence, is a normal Noetherian domain.* [AK21, (24.17)] [Rei95, p. 122] [Hoc17, p. 144]

We will use the following fact from field theory:

LEMMA 9.5.4. *Let $K \subseteq L$ be a finite field extension. Then, the following are equivalent:* [AK21, (24.15)] [Rei95, p. 125] [Hoc17, p. 147]

(*i*) *$K \subseteq L$ is separable.*
(*ii*) *The minimal polynomial of any element of L over K has no repeated roots.*
(*iii*) *The trace map $\mathrm{Tr}_{L/K} \colon L \to K$ is not identically zero, in which case*

$$\begin{aligned} L \times L &\longrightarrow K \\ (\ell_1, \ell_2) &\longmapsto \mathrm{Tr}(\ell_1 \ell_2) \end{aligned}$$

is a nondegenerate bilinear form.

The plan is to prove consequences of Lemma 9.5.4 to integral closure for now, and then go back and prove Lemma 9.5.4. In (*iii*), the *trace* of $\ell \in L$ is the trace of the K-vector space map $\ell \cdot - \colon L \to L$.

We start with the following important result.

[AK21, (24.16)] [Rei95, p. 123] [Hoc17, p. 144]

THEOREM 9.5.5. *Let R be a normal domain with fraction field K and let L be a finite extension of K. Let $s \in L$ be integral over R. Then, multiplication by s defines a K-linear map $L \to L$. The coefficients of the characteristic polynomial of this K-linear map are in R. In particular,*

$$\mathrm{Tr}_{L/K}(s) \in R.$$

Proof. We first consider the case when $L = K[s]$. By a preliminary result to Going Down (Proposition 4.7.3), we know that the minimal polynomial f for s in fact has coefficients in R. Suppose that f has degree d. Then, $[L : K] = d$, and the characteristic polynomial for the matrix defined by multiplication by s has degree d as well. Since the matrix satisfies this characteristic polynomial, so does s. Thus, the characteristic polynomial is equal to the minimal polynomial of s over K, and hence has coefficients in R.

In the general case, write $L_0 = K[s] \subseteq L$, let $v_1, \ldots, v_d$ be a basis for L_0 over K, and let $w_1, \ldots, w_h$ be a basis for L over L_0. Let A be the matrix of multiplication by s on L_0 with respect to the basis $v_1, \ldots, v_d$. Then, the span of $v_1 w_j, \ldots, v_d w_j$ is a $L_0 \cdot w_j$ and is stable under multiplication by s. We therefore see that the matrix of multiplication by s with respect to the basis

$$v_1 w_1, v_2 w_1, \ldots, v_d w_1, \ldots, v_1 w_h, v_2 w_1, \ldots, v_d w_h$$

is the direct sum of h copies of A, and its characteristic polynomial is f^h. We already know from the previous paragraph that it has coefficients in R. □

One consequence of Theorem 9.5.5 is Hochster's direct summand conjecture for $\mathbf{Q}$-algebras. Hochster's direct summand conjecture [Hoc73a, §0] says that if R is regular and $R \subseteq S$ is module-finite, then the map $R \to S$ has an R-linear retraction, in short, R is a direct summand of S. Hochster proved his direct summand conjecture for all regular rings containing a field [Hoc73a, Theorem 2]. Until fairly recently, the direct summand conjecture was only known in dimensions ≤ 3 in mixed characteristic. This case is due to Heitmann [Hei02]. The direct summand conjecture was shown in general by André [And18] using perfectoid spaces.

COROLLARY 9.5.6 [Hoc73a, Lemma 2]. *Let R be a normal domain that contains $\mathbf{Q}$, and let S be a module-finite extension of R. Then, R is a direct summand of S as an R-module. Hence, for every ideal $I \subseteq R$, we have $IS \cap R = I$.*

Proof. Since $R - \{0\}$ is multiplicative, there is a prime ideal $P \subseteq S$ disjoint from $R - \{0\}$. Thus, $R \hookrightarrow S/P$, which is still module-finite over R. It then suffices to show that $R \to S/P$ splits since the splitting ϕ composed with $S \twoheadrightarrow S/P$ would be a splitting of $R \to S$. Thus, we have reduced to the case when S is a module-finite extension domain of R.

Let $K = \operatorname{Frac}(R)$ and $L = \operatorname{Frac}(S)$ and let $n = [L : K]$. Then, $(1/n) \operatorname{Tr}_{L/K}$ when restricted to S takes values in R by Theorem 9.5.5, is R-linear, and is a splitting. □

Proof of Theorem 9.5.3. We proceed in a sequence of steps.

Step 1. Find $x_1, x_2, \ldots, x_n \in S$ that are a K-basis for L.

Let $\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$ be any K-basis for L. Each $\tilde{x}_i$ can be written as a fraction with denominator in S. By a step in our proof of Incomparability (Theorem 4.3.4(*i*)), we know that we can multiply the numerator and denominator by s/s for some $s \in S - \{0\}$ so that the denominator lies in R. Clearing denominators (which now lie in K), we have $x_i = b_i \tilde{x}_i \in S$ for some $b_i \in R$, which form a K-basis for L.

Step 2. We have $D = \det(\operatorname{Tr}_{L/K}(x_i x_j)) \in R$ and

$$DS \subseteq \sum_i R \cdot x_i.$$

Thus, S is module-finite and Noetherian over R.

The fact that $D \in R$ follows from Theorem 9.5.5, since all terms in the matrix are in R. The last statement then follows from the first two since

$$\begin{aligned} S &\xrightarrow{\sim} DS \\ s &\longmapsto Ds \end{aligned}$$

is an isomorphism of R-modules.

It remains to show that $DS \subseteq \sum_i R \cdot x_i$. Let $s \in S$. Then, $s \in L$ and hence can be written as $\alpha_1 x_1 + \cdots + \alpha_n x_n$. We may then multiply by $x_i \in S$ and take the trace of both sides to obtain

$$r_i \coloneqq \operatorname{Tr}_{L/K}(s x_i) = \sum_{j=1}^{n} \alpha_j \operatorname{Tr}_{L/K}(x_i x_j) \in R.$$

Let W be the column vector with entries r_i, and let V be the column vector with entries α_j. Then, $W = AV$, where $A = [\operatorname{Tr}_{L/K}(x_i x_j)]_{i,j}$ and W have entries in R. Let B be the classical adjoint of A, i.e., the transpose of the matrix of cofactors. Then, B also has entries in R, and $BA = D \cdot I_n$. It follows that

$$BW = BAV = DV,$$

and hence each $D\alpha_j$ is in R. But then,

$$Ds = (D\alpha_1)x_1 + \cdots + (D\alpha_n)x_n \in \sum_i R \cdot x_i,$$

as required. □

Corollary 9.5.7. *Let D be any Dedekind domain whose fraction field K is of characteristic zero, such as the integers. Let L be a finite algebraic extension of K. Then, the integral closure of D in L is module-finite over K, and hence is a Dedekind domain.* [AK21, (24.18)] [Rei95, p. 122] [Hoc17, p. 145]

Proof. By Theorem 9.5.3, the only thing remaining to check is that the dimension of the integral closure is 1. But this follows from the fact that integral extensions preserve dimension (Corollary 4.4.2). □

11/22

We now show that integral closures of finitely generated algebras over fields are Noetherian.

[AK21, (24.10)]
[Rei95, p. 122]
[Mat89, pp. 261–263]

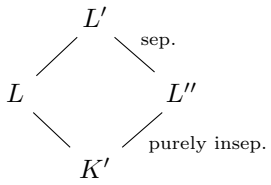
COROLLARY 9.5.8. *Let R be a domain finitely generated as an algebra over a field k. Let L be a finite algebraic extension of $K = \mathrm{Frac}(R)$. Then, the integral closure S of R in L is module-finite over R, and is therefore Noetherian.*

Proof. Consider a Noether normalization

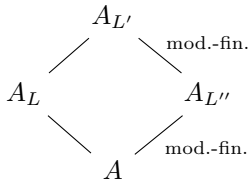
$$k \subseteq k[y_1, \dots, y_r] \subseteq R$$

for R. Then, S is the integral closure of $A = k[y_1, \dots, y_r]$ in L. Set $K' = \mathrm{Frac}(A) = k(y_1, \dots, y_r)$, in which case L is a finite algebraic extension of K'. If this extension is separable, then S is module-finite over A by Theorem 9.5.3.

Otherwise, suppose that L is inseparable over K', and let $p = \mathrm{char}(K)$. We consider the *normal closure* L' of L/K'. This field can be described as the splitting field of a set of minimal polynomials for generators of L/K', and by [Jac89, Proposition 8.14], we have the diagram



of field extensions. It therefore suffices to show that the integral closure $A_{L''}$ of A in L'' is finite over A, since then we would have a diagram



of integral closures of A in larger and larger fields where $A_{L'}$ is module-finite over $A_{L''}$ by Theorem 9.5.3, which shows that $A_{L'}$ is module-finite over A, and hence A_L is module-finite over A by the Noetherianity of $A_{L'}$ as an A-module (Proposition 6.2.7).

Since L'' is a finite purely inseparable extension of K', it is contained in a field L_0 that is obtained by adjoining to K' the q-th roots of a finite number of elements $a_1, \dots, a_s$ of k and also the q-th roots of $y_1, \dots, y_r$, where q is a sufficiently large power of p by [Jac89, Proposition 8.13]. Then, the integral closure of A in L_0 is

$$A_{L_0} = k'[y_1^{1/q}, \dots, y_r^{1/q}],$$

where $k' = k(a_1^{1/q}, \dots, a_s^{1/q})$, and this ring is module-finite over A since it is generated by ℓ-th powers of the elements $a_j^{1/q}$ and $y_i^{1/q}$, where $1 \leq \ell < q$. Since the integral closure $A_{L''}$ of A in L'' is contained in the integral closure A_{L_0} of A in L_0, we

see that $A_{L''}$ is module-finite over A by the Noetherianity of A_{L_0} as an A-module (Proposition 6.2.7). □

9.6. Classification of modules over a Dedekind domain (not covered in class)

We want to classify modules over a Dedekind domain, analogously to what one can do over a PID.

THEOREM 9.6.1. *Let R be a Dedekind domain and let M be a finitely generated R-module.* [Hoc17, pp. 149–150]

(a) *If M is torsion-free, then it is projective. In particular, every ideal of R is projective. The product IJ of two ideals $I, J \subseteq R$ satisfies*

$$IJ \cong I \otimes_R J$$

as R-modules, and hence its isomorphism class as an R-module depends only on the isomorphism classes of I and J as R-modules.

(b) *Given finitely many maximal ideals*

$$P_1, P_2, \ldots, P_k \subseteq R$$

and an ideal $I \neq 0$, the ideal I is isomorphic to an ideal not contained in any of the P_i.

(c) *M is a direct sum of a torsion module and a torsion-free module. The torsion submodule N is unique and may be viewed as a module over the localization of R along the complement of the union of finitely many maximal ideals in its support. This localization is a PID, and hence applying the classification of finitely generated modules over a PID, N is a direct sum of cyclic modules. The torsion-free summand of M is isomorphic to M/N.*

(d) *If $I, J \subseteq R$ are nonzero ideals, then*

$$I \oplus J \cong I \cap J \oplus (I + J) \cong IJ \oplus R$$

as R-modules. If $I_1, I_2, \ldots, I_n \subseteq R$ are nonzero ideals, then

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n \cong (I_1 I_2 \cdots I_n) \oplus R^{\oplus(n-1)}$$

as R-modules.

(e) *Any finitely generated torsion-free R-module M is the direct sum of a free R-module $R^{\oplus(n-1)}$ and an ideal $I \subseteq R$. The integer n is uniquely determined, and I is uniquely determined up to isomorphism as an R-module.*

Proof. (a). The localizations of R at maximal ideals are DVRs, and every finitely generated torsion-free module over a DVR is free by the classification of finitely generated modules over a PID [DF04, §12.1, Theorem 5(2)]. Since projective is equivalent to locally free by Corollary 7.10.3, we see that M is projective.

Now consider two ideals $I, J \subseteq R$. Tensoring the injection $J \subseteq R$ by I, we have an injection

$$I \otimes_R J \hookrightarrow I \otimes_R R \cong I$$

which is injective since I is projective and hence flat by Corollary 7.10.3. The image of this injection is IJ.

(b). Consider the multiplicative set

$$W = R - (P_1 \cup P_2 \cup \cdots \cup P_k).$$

Since $W^{-1}R$ is semi-local, $W^{-1}R$ is a PID by Homework 11, Problem 4(b). We therefore se that

$$IW^{-1}R = b\,W^{-1}R$$

for some $b \in I$. Thus, there exists $w \in W$ such that

$$wI \subseteq bR \subseteq I.$$

Dividing by b, we see that $J = (w/b)I \subseteq R$ is isomorphic to I as an R-module.

It remains to show that $J \not\subseteq P_i$ for all i. By way of contradiction, suppose that $J \subseteq P_i$ for some i. Then, we have $wI \subseteq bP_i$. Since $w \notin P_i$, we know that w becomes a unit after localizing at P_i. Thus, localizing at P_i, we have

$$bR_{P_i} = IR_{P_i} \subseteq bP_iR_{P_i}.$$

Dividing by b, we obtain $R_{P_i} \subseteq P_iR_{P_i}$, a contradiction.

(c). The torsion submodule N consists of all torsion elements in M, and is therefore unique. The quotient module M/N is torsion-free, since if an element $\bar{m} \in M/N$ is torsion, then $r\bar{m} = 0$ for some $r \in R$, which implies that $rm \in N$ and hence $m \in N$. By (a), we therefore see that M/N is projective, and hence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

is a split short exact sequence.

Now choose a finite set of generators for N. Each generator has a nonzero annihilator, and hence N also has a nonzero annihilator $\mathrm{Ann}_R(N)$. Letting $I = \mathrm{Ann}_R(N)$, we may view N as a module over R/I, which is a 0-dimensional Noetherian ring. The maximal ideals of R/I are the images of finitely many maximal ideals

$$P_1, P_2, \ldots, P_k \subseteq R.$$

Any element not in $P_1 \cup P_2 \cup \cdots \cup P_k$ acts as a unit on N, and hence N is a module over the localization of R at $R - (P_1 \cup P_2 \cup \cdots \cup P_k)$. We conclude that N is a direct sum of cyclic modules by the classification of finitely generated modules over a PID [DF04, §12.1, Theorem 5(1)].

(d). We have the short exact sequence

$$0 \longrightarrow I \cap J \xrightarrow{\begin{bmatrix} 1 \\ 1 \end{bmatrix}} I \oplus J \xrightarrow{[1\ -1]} I + J \longrightarrow 0.$$

Since $I + J$ is projective by (a), this short exact sequence splits, which shows that $I \oplus J \cong (I \cap J) \oplus (I + J)$. By ($b$), we can find an ideal $I' \subseteq R$ such that $I \cong I'$ as R-modules, but such that I' is not contained in any of the finitely many minimal primes of J. Thus, we see that I' and J are comaximal, i.e., $I' + J = R$, and hence $I' \cap J = I'J$ by the Chinese Remainder Theorem 4.5.5. We therefore have

$$\begin{aligned} I \oplus J &\cong I' \oplus J \\ &\cong (I' \cap J) \oplus (I' + J) \\ &= I'J \oplus R \\ &\cong (I' \otimes_R J) \oplus R \\ &\cong IJ \oplus R. \end{aligned}$$

The result for finitely many ideals now follows by induction on $n \geq 2$.

(*e*). Let $K = \mathrm{Frac}(R)$. Then, $K \otimes_R M \cong K^{\oplus n}$, and hence we can choose a nonzero map $K \otimes_R M \twoheadrightarrow K$. This map is an element of

$$\mathrm{Hom}_K(K \otimes_R M, K \otimes_R R) \cong K \otimes_R \mathrm{Hom}_R(M, R)$$

by the fact that Hom commutes with flat base change (Proposition 7.7.4). We therefore obtain a nonzero R-linear map $f\colon M \to R$. Let $I = f(M)$, which is an ideal of R. By (*a*), we know that I is projective. The map $M \twoheadrightarrow I$ therefore splits, and hence $M \cong M_0 \oplus I$ where $M_0 = \ker(M \twoheadrightarrow I)$. Iterating, we see that M is a direct sum of ideals $I_1 \oplus I_2 \oplus \cdots \oplus I_n$. By (*d*), we know that

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n \cong R^{\oplus(n-1)} \oplus (I_1 I_2 \cdots I_n).$$

The integer n is the torsion-free rank of M, i.e., the K-vector space dimension of $K \otimes_R M$.

It remains to show that the R-module isomorphism class of the ideal $I_1 I_2 \cdots I_n$ is unique. This follows from Lemma 9.6.2 below. □

LEMMA 9.6.2. *Let R be a Noetherian ring and let P, P' be finitely generated R-modules that are locally free of rank 1. Suppose that* [Hoc17, p. 151]

$$M = R^{\oplus(n-1)} \oplus P \cong R^{\oplus(n-1)} \oplus P'.$$

Then, $P \cong P'$.

Proof. Taking exterior powers, we obtain

$$P \cong \bigwedge_R^n M \cong P'. \qquad \square$$

CHAPTER 10

Completions

The last topic that will appear on the final exam is completions.

10.1. Motivation

We saw already how localization can tell us "local" information on an algebraic set. For example, denoting by k a field of characteristic $\neq 2$, the ring

$$\frac{k[x,y]}{(y^2 - x^2(x+1))}$$

is a domain, but you saw on homework that

$$\frac{k[\![x,y]\!]}{(y^2 - x^2(x+1))}$$

is not. This is because formal power series are able to see some extra "analytic" phenomena.

These two rings are connected by a process called *completion*. Our goal in this chapter will be to introduce this concept and see how it affects properties of rings and modules.

10.2. Direct limits and inverse limits

Completions will be defined as a special case of an inverse limit. To help us think about limits, we start by defining direct limits and inverse limits and giving some examples.

DEFINITION 10.2.1 (Filtered partially ordered set). A partially ordered set $(I, \leq)$ is *filtered* or *directed* if, for any two elements $i, j \in \Lambda$, there exists $k \in \Lambda$ with $i \leq k$ and $j \leq k$. In other words, any two elements of I have an upper bound in a filtered partially ordered set. [Hoc17, p. 153]

EXAMPLES 10.2.2. Here are examples of filtered partially ordered sets. [Hoc17, p. 153]

(1) Totally ordered sets, for example, the natural numbers $\mathbf{N}$ and the positive integers.
(2) Finite subsets of a given set under $\subseteq$.
(3) Finitely generated R-submodules of an R-module under $\subseteq$.
(4) Finitely generated R-subalgebras of an R-algebra under $\subseteq$.
(5) Open neighborhoods of a point $x \in X$, where X is a topological space, under $\supseteq$.

We now define direct systems and direct limits.

Definition 10.2.3 (Direct system). Let $(I, \leq)$ be a partially ordered set. A *direct system* or *direct limit system* indexed by I in a category $\mathcal{C}$ is a functor $I \to \mathcal{C}$ where I is considered as a category as in Example 2.1.2(6). Explicitly, for every element $i \in I$, we have an object X_i in $\mathcal{C}$, and for all pairs $i, j \in I$, we have a morphism [Hoc17, p. 153]

$$f_{ij} \colon X_i \longrightarrow X_j$$

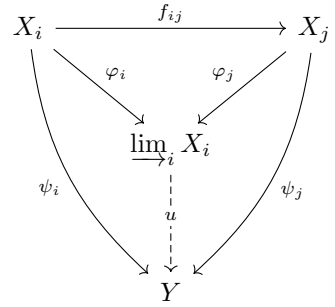
such that

(1) $f_{ii} = \mathrm{id}_{X_i}$ for every $i \in I$.
(2) Whenever $i \leq j \leq k$, we have $f_{ik} = f_{jk} \circ f_{ij}$.

If I is filtered, we say that the direct system is a *filtered direct system*.

[Hoc17, p. 153] [Lan02, Thm. III.10.1]

Definition 10.2.4 (Direct limit). Let $\{X_i, f_{ij}\}$ be a direct system of objects and morphisms in a category $\mathcal{C}$. The *direct limit* of the system $\{X_i, f_{ij}\}$ is an object of $\mathcal{C}$ denoted by $\varinjlim X_i$ with *insertion morphisms* $\{\varphi_i \colon X_i \to \varinjlim X_i\}$ such that $\varphi_j \circ f_{ij} = \varphi_i$ for all $i \leq j$. Moreover, if $Y \in \mathcal{C}$ is another object with morphisms $\{\psi_i \colon X_i \to Y\}$ such that $\psi_j \circ f_{ij} = \psi_i$ for all $i \leq j$, then there is a unique morphism $u \colon \varinjlim X_i \to Y$ making the following diagram commute:



If the direct system is filtered, we call the direct limit a *filtered direct limit*.

Examples 10.2.5. Let $\mathcal{C}$ be the category of sets, groups, Abelian groups, rings, R-modules, or R-algebras. (The examples below will work for any category where the objects have an underlying set and a morphism is a function possibly satisfying additional conditions.)

[Hoc17, p. 154]

(1) Let Z be a fixed object in $\mathcal{C}$ and let $\{X_i\}$ be a filtered set of subobjects of Z, partially ordered by inclusion. Then, the direct limit of the X_i is the union of these subobjects, and is called the *filtered union*.

[Hoc17, p. 154] [AK21, (7.4)]

(2) Let $\{X_i, f_{ij}\}$ be a filtered direct system of objects and morphisms in $\mathcal{C}$. Then, the filtered direct limit exists and can be constructed as

$$\varinjlim_i X_i \coloneqq \bigsqcup_i X_i \Big/ f_{ij}(x) \sim x \text{ for all } i \leq j.$$

If $\mathcal{C}$ is the category of Abelian groups or R-modules, then the direct limit exists and can be constructed as

$$\varinjlim_i X_i \coloneqq \bigoplus_i X_i \Big/ \big(f_{ij}(x) - x\big)_{i \leq j}$$

where $(f_{ij}(x) - x)_{i \leq j}$ is the subobject generated by the elements $f_{ij}(x) - x$.

For the next example, we need the universal property of localization of modules, which we did not state explicitly before.

THEOREM 10.2.6. *Let R be a ring and consider a multiplicative set $W \subseteq R$. Let $\varphi\colon M \to T$ be an R-module map such that T is an $W^{-1}R$-module. Then, there is a unique R-module map $\tilde{\varphi}\colon W^{-1}M \to T$ making the diagram* [AK21, (12.3)]

$$\begin{array}{ccc} M & \xrightarrow{\ell_W} & W^{-1}M \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \exists!} \\ & & T \end{array}$$

commute. In other words, $W^{-1}M$ represents the functor

$$\begin{aligned} \mathsf{Mod}_{W^{-1}R} &\longrightarrow \mathsf{Sets} \\ T &\longmapsto \mathrm{Hom}_R(M, T). \end{aligned}$$

Proof. We have the isomorphisms of functors

$$\begin{aligned} \mathrm{Hom}_{W^{-1}R}(W^{-1}M, -) &\xrightarrow{\sim} \mathrm{Hom}_{W^{-1}R}(W^{-1}R \otimes_R M, -) \\ &\xrightarrow{\sim} \mathrm{Hom}_R\big(M, \mathrm{Hom}_{W^{-1}R}(W^{-1}R, -)\big) \\ &\xleftarrow{\sim} \mathrm{Hom}_R(M, -) \end{aligned}$$

by Proposition 7.4.5, tensor–Hom adjunction (Theorem 7.6.1), and the isomorphism of functors

$$\mathrm{id}_{\mathsf{Mod}_{W^{-1}R}} \xrightarrow{\sim} \mathrm{Hom}_{W^{-1}R}(W^{-1}R, -).$$

Alternatively, see [AK21, (12.3)] for a direct proof. □

We now give an important example of a direct limit.

EXAMPLE 10.2.7 (Principal localization as a direct limit). For a specific example, let R be a ring and let $f \in R$ be an element. Consider the direct system containing all compositions of maps appearing in the sequence [EGAI, (**0**, 1.6)] [EGAI$_{\text{new}}$, (**0**, 6.2)]

$$M \xrightarrow{f\cdot -} M \xrightarrow{f\cdot -} M \xrightarrow{f\cdot -} \cdots$$

of R-modules. Denoting by M_i the i-th term of this direct system where $i \in \mathbf{N} = \{0, 1, 2 \ldots\}$, the transition maps are

$$f_{ij}\colon M_i \xrightarrow{f^{j-i}\cdot -} M_j$$

for all $i \leq j$. If we think about the direct limit as

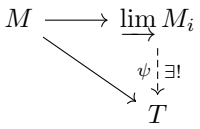
$$\varinjlim_i M_i \cong \bigoplus_i M_i \Big/ \big(f_{ij}(x) - x\big)_{i \leq j},$$

we can give $\varinjlim M_i$ the structure of a R_f-module by saying that

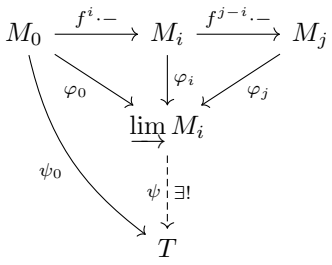
$$\frac{r}{f^j} \cdot \bar{m}_i = \overline{f_{ij}(rm_i)}$$

where $\bar{m}_i$ is the image of $m_i \in M_i$ in $\varinjlim M_i$.

We now consider the commutative diagram



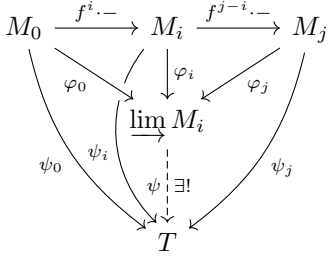
for an R_f-module T. We must show that a dashed map of R_f-modules exists that is the unique map making the diagram commute. We enlarge the commutative diagram to include the direct system $\{M_i\}$:



Now for each $m_i \in M_i$, we can map it to an element of T by sending

$$\begin{aligned} \psi_i \colon M_i &\longrightarrow T \\ m_i &\longmapsto \frac{\psi_0(m_i)}{f^i}. \end{aligned}$$

This is an R-module map since it is $(f^{-i} \cdot -) \circ \psi_0$ and commutes with the transition maps in the direct system $\{M_i\}$:



By the universal property of direct limits, the dashed map $\psi \colon \varinjlim M_i \to T$ exists and is the unique map making the diagram commute.

Finally, we check that the map ψ is a map of R_f-moules. If $\bar{m}_i$ is the image of $m_i \in M_i$ in $\varinjlim M_i$, we have

$$\psi\left(\frac{r}{f^j} \cdot \bar{m}_i\right) = \psi_j\big(\overline{f_{ij}(rm_i)}\big) = \frac{\psi_0(rm_i)}{f^j} = \frac{r}{f^j} \cdot \psi(\bar{m}_i).$$

Thus, M_f is the direct limit of the direct system $\{M_i\}$ by the Yoneda Lemma 4.6.1.

Next, we define inverse systems and inverse limits.

[Hoc17, p. 155] Definition 10.2.8 (Inverse system). Let $(I, \leq)$ be a partially ordered set. An *inverse system* or *inverse limit system* indexed by I in a category $\mathcal{C}$ is a functor $I^{\mathrm{op}} \to \mathcal{C}$ where I is considered as a category as in Example 2.1.2(6). Explicitly, for

every element $i \in I$, we have an object X_i in $\mathcal{C}$, and for all pairs $i, j \in I$, we have a morphism

$$f_{ij} \colon X_j \longrightarrow X_i$$

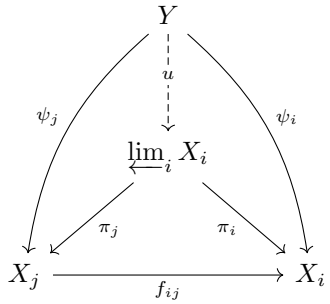
such that

(1) $f_{ii} = \mathrm{id}_{X_i}$ for every $i \in I$.
(2) Whenever $i \leq j \leq k$, we have $f_{ik} = f_{ij} \circ f_{jk}$.

If I is filtered, we say the inverse system is a *cofiltered inverse system*.

11/25

DEFINITION 10.2.9 (Inverse limit). Let $\{X_i, f_{ij}\}$ be a inverse system of objects and morphisms in a category $\mathcal{C}$. The *inverse limit* of the system $\{X_i, f_{ij}\}$ is an object of $\mathcal{C}$ denoted by $\varprojlim X_i$ with morphisms $\{\pi_i \colon \varprojlim X_i \to X_i\}$ such that $f_{ij} \circ \pi_j = \pi_i$ for all $i \leq j$. Moreover, if Y is another object with morphisms $\{\psi_i \colon Y \to X_i\}$ such that $f_{ij} \circ \psi_j = \psi_i$ for all $i \leq j$, then there is a unique morphism $u \colon Y \to \varprojlim X_i$ making the following diagram commute: [Hoc17, p. 155]



If I is filtered, we say the inverse limit is a *cofiltered inverse limit*.

EXAMPLE 10.2.10. Let $\mathcal{C}$ be the category of sets, Abelian groups, rings, R-modules, or R-algebras. The inverse limit exists and can be constructed as [Hoc17, pp. 155–156]

$$\varprojlim_i X_i \coloneqq \left\{ (x_1, x_2, \ldots) \in \prod_i X_i \;\middle|\; f_{ij}(x_j) = x_i \text{ for all } i \leq j \right\}.$$

10.3. Completions of rings and modules

Our goal now is to define completions topologically and to describe it as an inverse limit. The construction might look familiar to you as being similar to the construction of real numbers as equivalence classes of Cauchy sequences of rational numbers.

DEFINITION 10.3.1. Let R be a ring and let $I \subseteq R$ be an ideal. Let M be an R-module. Consider the set of all sequences of elements in M indexed by $\mathbf{N}$ under termwise addition. This ring is the same as a direct product of countably many copies of M. [Hoc17, p. 156, pp. 158–159]

The R-submodule $\mathfrak{C}_I(M)$ of *Cauchy sequences for the I-adic topology* consists of those sequences $m_0, m_1, \ldots$ such that for all $t \in \mathbf{N}$, there exists $N \in \mathbf{N}$ such that $m_i - m_j \in I^t M$ for all $i, j \geq N$. There is a map

$$\begin{aligned} M &\longrightarrow \mathfrak{C}_I(M) \\ m &\longmapsto (m, m, \ldots). \end{aligned}$$

If $M = R$, the module $\mathfrak{C}_I(M)$ is an R-algebra by defining multiplication termwise and using the map

$$\begin{aligned} R &\longrightarrow \mathfrak{C}_I(R) \\ r &\longmapsto (r, r, \ldots) \end{aligned}$$

to define the R-algebra structure.

Let $\mathfrak{C}_I^0(M)$ be the set of *null sequences*, which by definition consists of those sequences $m_0, m_1, \ldots$ such that for all $t \in \mathbf{N}$, there exists $N \in \mathbf{N}$ such that $m_i \in I^t M$ for all $i \geq N$. Then, $\mathfrak{C}_I^0(M)$ is an ideal in $\mathfrak{C}_I(M)$, and we can define the *I-adic completion of M* as

$$\widehat{M}^I \coloneqq \frac{\mathfrak{C}_I(M)}{\mathfrak{C}_I^0(M)}.$$

This is the same as taking the quotient of $\mathfrak{C}_I(M)$ by the equivalence relation where $(m_i)_{i\in\mathbf{N}} \sim (n_i)_{i\in\mathbf{N}}$ if and only if for every $t \in \mathbf{N}$, we have $m_i - n_i \in I^t M$ for sufficiently large i. Since $\mathfrak{C}_I^0(R)\,\mathfrak{C}_I(M) \subseteq \mathfrak{C}_I^0(M)$, the module $\widehat{M}^I$ has the structure of an $\widehat{R}^I$-module.

We have a map

$$M \longrightarrow \widehat{M}^I,$$

which has kernel $\bigcap_{t\in\mathbf{N}} I^t M$. We say that M is *I-adically separated* if $M \to \widehat{M}^I$ is injective. We say that M is *I-adically complete* if $M \to \widehat{M}^I$ is an isomorphism. Note that M is I-adically separated if and only if every Cauchy sequence is the sum of a constant sequence $r, r, \ldots$ and a null sequence.

[AM69, Cor. 10.18]

Example 10.3.2. Note that

$$\ker\bigl(R \longrightarrow \widehat{R}^I\bigr) = \bigcap_{t\in\mathbf{N}} I^t.$$

On Homework 11, Problem 1(f), you showed that if R is a Noetherian domain and I is a proper ideal, then $\bigcap_t I^t = 0$. Thus, in this case R is I-adically separated.

[Hoc17, pp. 157–158]

Remark 10.3.3 (Connection to Cauchy completion of metric spaces). Let M be an I-adically separated module. Fix a real number $\delta \in (0, 1)$. We define the distance $d(m, n)$ between two elements $m, n \in M$ as

$$d(m,n) \coloneqq \begin{cases} \delta^{\max\{t \mid m-n \in I^t M\}} & \text{if } m \neq n, \\ 0 & \text{if } m = n. \end{cases}$$

This is a metric on M: The triangle inequality holds for ℓ, m, n if any two elements are equal, and otherwise, if $\ell - m \in I^s, m - n \in I^t, n - \ell \in I^u$, then since

$$n - \ell = -(\ell - m) - (m - n),$$

we know that $u \geq \min\{s, t\}$ with equality unless $s = t$. Thus, the notion of completion we have defined is literally the same as the one from analysis.

By construction, for any element of $\mathfrak{C}_I(M)$, we can consider the residue modulo $I^t M$ for a given t. By the definition of a Cauchy sequence, these residues are eventually all the same. By taking these residues, we obtain a map

$$\begin{aligned} \mathfrak{C}_I(M) &\longrightarrow M/I^t M \\ (m_0, m_1, \ldots) &\longmapsto \text{stable image of the } m_i \end{aligned}$$

that kills $\mathfrak{C}^0(M)$. Thus, for all t, we have surjections

$$\widehat{M}^I \twoheadrightarrow M/I^tM.$$

By the universal property of inverse limits in the category of R-modules, we have an R-module map

$$\widehat{M}^I \longrightarrow \varprojlim_t M/I^tM.$$

Similarly, if $M = R$, we have a map of R-algebras

$$\widehat{R}^I \longrightarrow \varprojlim_t R/I^t.$$

THEOREM 10.3.4. *Let R be a ring and let I be an ideal. Let M be an R-module. Then, the map* [Hoc17, p. 157]

$$\widehat{M}^I \longrightarrow \varprojlim_t M/I^tM$$

of R-modules induced by the universal property of inverse limits is a bijection.

Proof. For surjectivity, suppose we have a sequence $(m_i)_{i\in\mathbf{N}} \in \varprojlim_i M_i$ represented by a sequence $(\tilde{m}_i)_{i\in\mathbf{N}} \in \prod_i M_i$. Then, the sequence $(\tilde{m}_i)_{i\in\mathbf{N}}$ forms a Cauchy sequence in M since

$$\tilde{m}_i - \tilde{m}_j \in I^{\min\{i,j\}}$$

for every $i, j \in \mathbf{N}$.

For injectivity, suppose we have another sequence $(\tilde{n}_i)_{i\in\mathbf{N}} \in \prod_i M_i$ mapping to the same element in $\varprojlim_i M_i$. Then, the sequence

$$\left(\tilde{m}_i - \tilde{n}_i\right)_{i\in\mathbf{N}}$$

must have terms in I^tM for all t, and hence represents the null sequence in M. □

REMARK 10.3.5 ("Standard" Cauchy sequences). You can think of $\widehat{R}^I$ as consisting of "formal power series in I": an element $r \in \widehat{R}^I$ can be written as [Hoc17, p. 157]

$$\underset{\in R}{r_0} + \underset{\in I}{r_1} + \underset{\in I^2}{r_2} + \cdots + \underset{\in I^t}{r_t} + \cdots$$

corresponding to the sequence

$$r_0, r_0 + r_1, r_0 + r_1 + r_2, \ldots, r_0 + \cdots + r_t, \ldots.$$

To do this for a sequence (s_n), you can first pass to a subsequence such that for every $t \in \mathbf{N}$, the residue of r_k in R/I^t is the same for all $k \geq t$. You can then write

$$s_0 + (s_1 - s_0) + (s_2 - s_1) + \cdots$$

to get a sequence of the required form.

We now have a natural surjective map

$$\widehat{R}^I \twoheadrightarrow R/I$$
$$(r_0, r_1, \ldots) \longmapsto \text{stable image of the } r_i.$$

The kernel J is represented by Cauchy sequences all of whose terms are in I.

PROPOSITION 10.3.6. *Let R be a ring and let $I \subseteq R$ be an ideal. Set* [Hoc17, p. 157]

$$J \coloneqq \ker\big(\widehat{R}^I \twoheadrightarrow R/I\big).$$

Then, every element $u + j \in \widehat{R}^I$ where u is a unit and $j \in J$ is invertible in $\widehat{R}^I$. Moreover, J is contained in every maximal ideal of $\widehat{R}^I$, and hence there is a bijection

$$\big\{\textit{maximal ideals in } \widehat{R}^I\big\} \longleftrightarrow \big\{\textit{maximal ideals in } R/I\big\}.$$

In particular, if R/I is local, then $\widehat{R}^I$ is local.

Proof. We can write $u + j = u(1 + u^{-1}j)$, and hence it suffices to show that $1 + j$ is invertible for all $j \in J$. Let $(r_0, r_1, \ldots)$ be a Cauchy sequence representing j such that $r_i \in I$ for all i. From calculus, we know that

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots.$$

We are therefore led to consider the sequence

$$1 - r_0, 1 - r_1 + r_1^2, \ldots, \underbrace{1 - r_n + r_n^2 - r_n^3 + \cdots + (-1)^{n+1} r_n^{n+1}}_{=:s_n}.$$

If $r_n - r_{n+1} \in I^t$, then

$$s_n - s_{n+1} = (-1)^{n+2}\, r_{n+1}^{n+2} + \sum_{i=0}^{n} (-1)^{i+1}\big(r_n^{i+1} - r_{n+1}^{i+1}\big) \in I^{n+2} + I^t$$

since each of the terms $r_n^{i+1} - r_{n+1}^{i+1}$ are divisible by $r_n - r_{n+1} \in I^t$. Thus, the sequence (s_n) is Cauchy. We also have

$$1 - (1 + r_n)s_n = r_n^{n+2}$$

which is a null sequence, and hence (s_n) represents an inverse for $1 + j$ in $\widehat{R}^I$.

For the last statement, suppose $\mathfrak{m} \subseteq \widehat{R}^I$ is a maximal ideal that does not contain an element $j \in J$. Then, we have $J + \mathfrak{m} = R$ by maximality of $\mathfrak{m}$, and hence $j + x = 1$ for some $j \in J$ and $x \in \mathfrak{m}$. But then, the unit $1 - j = x$ lies in $\mathfrak{m}$, which is a contradiction. The bijection follows from Proposition 1.3.12. □

We now compute a particularly important example: the formal power series ring.

[Hoc17, p. 158] EXAMPLE 10.3.7 (Formal power series rings). Let R be a ring. Consider the polynomial ring $S = R[x_1, x_2, \ldots, x_n]$ and let $I = (x_1, x_2 \ldots, x_n)S$. An element of S/I^n is represented by a polynomial of degree $\leq n - 1$ in the x_i, and a sequence of such polynomials represents an element of the inverse limit if and only if the n-th term is equal to the sum of the terms of degree at most n in the $n + 1$-st term. Thus, we have

$$\widehat{S}^I \cong R[\![x_1, x_2, \ldots, x_n]\!].$$

12/2 Using this example we can make precise what we said before about completions being "more local".

EXAMPLE 10.3.8. Proposition 10.3.6 shows that if $\mathfrak{m} \subseteq R$ is maximal, then $\widehat{R}^{\mathfrak{m}}$ is local, and there is a commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & \widehat{R}^{\mathfrak{m}} \\ & \searrow \quad \nearrow & \\ & R_{\mathfrak{m}} & \end{array}$$

For example, if $R = k[x_1, \ldots, x_n]$ and $\mathfrak{m} = (x_1, \ldots, x_n)$, then $\widehat{R}^{\mathfrak{m}} = k[\![x_1, \ldots, x_n]\!]$, and there is a nice factorization of the map $k[x_1, \ldots, x_n] \to k[\![x_1, \ldots, x_n]\!]$ through the localization. This is one sense in which completions are "more local" than localizations. Similarly, the p-adic integers $\hat{\mathbf{Z}}_p$ coincide with the (p)-adic completion of $\mathbf{Z}_{(p)}$.

For a concrete example, consider the (x, y)-adic completion of

$$\frac{k[x, y]}{(y^2 - x^2(x+1))}$$

when $\operatorname{char}(k) \neq 2$. The (x, y)-adic completion ends up being the same thing as

$$\frac{k[\![x, y]\!]}{(y^2 - x^2(x+1))}.$$

Now recall that $\sqrt{x+1}$ has the Taylor series expansion

$$\sqrt{x+1} \approx 1 + \frac{x}{2} - \frac{x^2}{8} + \frac{x^3}{16} - \cdots,$$

which is a formal power series, and hence we can factor $y^2 - x^2(x+1)$ as

$$\left(y + x\left(1 + \frac{x}{2} - \frac{x^2}{8} + \frac{x^3}{16} - \cdots\right)\right)\left(y - x\left(1 + \frac{x}{2} - \frac{x^2}{8} + \frac{x^3}{16} - \cdots\right)\right).$$

Thus, $k[\![x, y]\!]/(y^2 - x^2(x+1))$ is not a domain!

We want to understand how completions behave with respect to ring maps.

DISCUSSION 10.3.9. Let $\varphi\colon R \to R'$ be a ring map. Consider ideals $I \subseteq R$ and $I' \subseteq R'$ such that $\varphi(I) \subseteq I'$. Then, sequences in R with respect to I map to Cauchy sequences in R' with respect to I', and null sequences map to null sequences. Thus, we get an induced ring map [Hoc17, p. 158]

$$\widehat{R}^I \longrightarrow \widehat{R'}^{I'}.$$

This construction is functorial in the sense that if we have another ring map $\psi\colon R' \to R''$ together with an ideal I'' such that $\psi(I') \subseteq I''$, then

$$\widehat{R}^I \longrightarrow \widehat{R'}^{I'} \longrightarrow \widehat{R''}^{I''}$$

is the same map as the map

$$\widehat{R}^I \longrightarrow \widehat{R''}^{I''}$$

defined by the procedure above.

If $\varphi\colon R \to R'$ is surjective and $\varphi(I) = I'$, then the map of completions is surjective: Each element of $\widehat{R'}^{I'}$ can be represented as partial sums of a series

$$s_0 + s_1 + s_2 + \cdots$$

where $s_n \in (I')^n$, but each I^n maps onto $(I')^n$, and hence we can find $r_n \in I^n$ mapping to each s_n. The series

$$r_0 + r_1 + r_2 + \cdots$$

represents an element of $\widehat{R}^I$ that maps onto $s_0 + s_1 + s_2 + \cdots$.

Combining Discussion 10.3.9 and Example 10.3.7 from last time, we obtain the following important consequence:

[Hoc17, p. 158] THEOREM 10.3.10. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Then, $\widehat{R}^I$ is Noetherian.*

Proof. Write $I = (f_1, f_2, \ldots, f_n)$. Map

$$\begin{aligned} R[x_1, \ldots, x_n] &\longrightarrow R \\ x_i &\longmapsto f_i \end{aligned}$$

as an R-algebra. This is surjective and $(x_1, x_2, \ldots, x_n)S$ maps onto I. We therefore have a surjective map

$$\begin{aligned} R[\![x_1, \ldots, x_n]\!] &\twoheadrightarrow \widehat{R}^I \\ x_i &\longmapsto f_i \end{aligned}$$

by Discussion 10.3.9. The ring $R[\![x_1, \ldots, x_n]\!]$ is Noetherian by Theorem 6.10.1, and hence $\widehat{R}^I$ is also Noetherian. □

[Hoc17, p. 159] LEMMA 10.3.11. *The I-adic completion for modules is a functor*

$$\mathsf{Mod}_R \longrightarrow \mathsf{Mod}_{\widehat{R}^I}$$

that takes surjections to surjections.

Proof. The proof is very similar to Discussion 10.3.9.

The first statement follows by the fact that if $h\colon M \to N$ is an R-module map, then $h(I^t M) = I^t N$ for every $t \in \mathbf{N}$.

For the second statement, consider a map $M \to Q$. Let $z \in \widehat{Q}^I$ be an element represented by the partial sums of a formal series

$$q_0 + q_1 + q_2 + \cdots$$

where $q_t \in I^t Q$. Now for all t, $I^t M$ maps onto $I^t Q$. Thus, we can find $u_t \in I^t M$ mapping onto q_t for every t, and the partial sums of

$$u_0 + u_1 + u_2 + \cdots$$

represent a Cauchy sequence mapping to z. □

10.4. The Artin–Rees lemma

We now note that $\widehat{M}^I$ is an R-module by restriction of scalars, and there is a natural R-linear map $M \to \widehat{M}^I$ sending u to the constant Cauchy sequence $u, u, \ldots$. By tensor–Hom adjunction (Corollary 7.6.2), there is therefore an $\widehat{R}^I$-linear map

$$\widehat{R}^I \otimes_R M \longrightarrow \widehat{M}^I.$$

The following facts are known about this map:

(1) If R is Noetherian and M is finitely generated, then
$$\widehat{R}^I \otimes_R M \xrightarrow{\sim} \widehat{M}^I$$
is an isomorphism.
(2) If R is Noetherian, then the restriction of the functor
$$\mathsf{Mod}_R \longrightarrow \mathsf{Mod}_{\widehat{R}^I}$$
to finitely generated modules is exact.
(3) If R is Noetherian, then $\widehat{R}^I$ is flat over R. In particular, if $(R, \mathfrak{m})$ is Noetherian and local, then $\widehat{R}^{\mathfrak{m}}$ is local and is faithfully flat over R.

To prove these properties, we need to prove the Artin–Rees lemma. An important construction that is needed to prove this result is the following construction due to Rees.

Definition 10.4.1 (Rees algebras [Ree56b, p. 222]). Let R be a ring and let $I \subseteq R$ be an ideal. Let t be an indeterminate and set [Hoc17, p. 159]
$$I^n t^n \coloneqq \left\{ it^n \;\middle|\; i \in I^n \right\} \subseteq R[t].$$
The *Rees algebra* or *Rees ring of* I is
$$R[It] \coloneqq R \oplus \bigoplus_{n=1}^{\infty} I^n t^n \subseteq R[t].$$

Note that if M is an R-module and t is an indeterminate, then every element of $R[t] \otimes_R M$ can be written uniquely in the form
$$1 \otimes u_0 + t \otimes u_1 + \cdots + t^k \otimes u_k \in R[t] \otimes_R M$$
where $u_j \in M$ for sufficiently large k. This is because if a larger s is used, then one has $m_{k+1} = \cdots = m_s = 0$. We will often use the notation
$$u_0 + u_1 t + \cdots + u_k t^k \in M[t]$$
for this element instead because it looks like a polynomial in t with coefficients in M. This notation helps us keep track of the graded $R[t]$-module structure on $M[t]$:
$$(rt^j)(ut^k) = (ru)t^{j+k}.$$

We now state the Artin–Rees lemma. Sharp [Sha16, p. 388] recounts the history of the result as told to him by Rees as follows. Rees had the proof of the lemma in 1954, but did not submit [Ree56a] for publication until May 1955. Around the same time, Emil Artin had proved the same result, and (for example) lectured on this result at Kyoto University on September 23, 1955 [Yos57, p. 35; Nag75, p. 212]. Sharp continues: "Nagata was asked to adjudicate as to who should receive the credit, and responded that 'it is obviously the Artin–Rees Lemma' " [Sha16, p. 388].

Theorem 10.4.2 (The Artin–Rees lemma [Ree56a, Lemma 1]). *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. Let $N \subseteq M$ be Noetherian modules. Then, there is a constant positive integer c such that for all $n \geq c$, we have* [Hoc17, p. 160]
$$I^n M \cap N = I^{n-c}(I^c M \cap N).$$
In other words, eventually, each of the modules $N_{n+1} = I^{n+1}M \cap N$ is I times its predecessor $N_n = I^n M \cap N$.

In particular, there is a constant c such that
$$I^n M \cap N \subseteq I^{n-c} N.$$

Thus, if a sequence of elements in N is an I-adic Cauchy sequence in M (resp. is a null sequence in M), then it is an I-adic Cauchy sequence in N (resp. is a null sequence in N).

Proof. Consider the module $R[t] \otimes_R M$, which we think of as $M[t]$ as above. Within this module, the submodule

$$\mathcal{M} = M \oplus \bigoplus_{n=1}^{\infty} I^n M t^n = M \oplus IMt \oplus I^2 M t^2 \oplus \cdots \oplus I^k M t^k \oplus \cdots$$

is a finitely generated $R[It]$-module, generated by the same set of generators as M as an R-module. Thus, $\mathcal{M}$ is finitely generated over $R[It]$. Since $R[It]$ is Noetherian (if $I = (x_1, x_2, \ldots, x_r)$, then $R[It]$ is finitely generated by $x_1 t, x_2 t, \ldots, x_r t$ as an R-algebra), we see that $\mathcal{M}$ is Noetherian. The sub-$R[t]$-module

$$\mathcal{N} = N[t] \cap \mathcal{M} = N \oplus (IM \cap N)t \oplus (I^2 M \cap N)t^2 \oplus \cdots$$

of $\mathcal{M}$ is therefore finitely generated over $R[It]$. Thus, for some $c \in \mathbf{N}$, we can choose a finite set of generators whose degrees in t are all at most c. By breaking the generators up into summands that are homogeneous with respect to t, we see that we may use elements from

$$N, (IM \cap N)t, (I^2 M \cap N)t^2, \ldots, (I^c M \cap N)t^c \tag{10.4.3}$$

as generators.

Now suppose that $n \geq c$ and that $u \in I^n M \cap N$. Then, ut^n can be written as an $R[It]$-linear combination of elements from (10.4.3), and hence as a sum of terms of the form

$$i_h t^h v_j t^j = (i_h v_j) t^{h+j}$$

where $j \leq c$, $i_h \in I^h$, and $v_j \in I^j M \cap N$, where $h + j = n$. This shows that

$$I^n M \cap N = \sum_{j \leq c} I^{n-j}(I^j M \cap N). \tag{10.4.4}$$

But

$$\begin{aligned} I^{n-j}(I^j M \cap N) &= I^{n-c} I^{c-j}(I^j M \cap N) \\ &\subseteq I^{n-c}(I^c M \cap N) \end{aligned}$$

and hence we only need the single term $I^{n-c}(I^c M \cap N)$ in the sum (10.4.4). □

As a consequence, we have the following.

[Hoc17, p. 161]

THEOREM 10.4.5. *Let R be a Noetherian ring and let $I \subseteq R$ be an ideal.*

(*a*) *If $0 \to N \to M \to Q \to 0$ is a short exact sequence of finitely generated R-modules, then the sequence*

$$0 \longrightarrow \widehat{N}^I \longrightarrow \widehat{M}^I \longrightarrow \widehat{Q}^I \longrightarrow 0$$

is exact. In other words, I-adic completion is an exact functor on finitely generated R-modules.

(*b*) *The natural transformation θ from $\widehat{R}^I \otimes_R -$ to the I-adic completion functor is an isomorphism of functors on finitely generated R-modules. In other words, for every finitely generated R-module M, the natural map*

$$\theta_M \colon \widehat{R}^I \otimes_R M \longrightarrow \widehat{M}^I$$

is an isomorphism.

(*c*) $\widehat{R}^I$ *is a flat* R*-algebra. If* $(R, \mathfrak{m})$ *is local,* $\widehat{R} = \widehat{R}^{\mathfrak{m}}$ *is a faithfully flat local* R*-algebra.*

Proof. (*a*). We already know that $\widehat{M}^I \to \widehat{Q}^I$ is surjective. Now let $y \in \widehat{M}^I$ map to 0 in $\widehat{Q}^I$. Choose a Cauchy sequence $u_0, u_1, u_2, \ldots$ that represents y. After passing to a subsequence, we may assume that

$$u_t - u_{t+1} \in I^t M$$

for every t. Then, the images of u_t in $Q \cong M/N$ converge to 0. Passing to a further subsequence we may assume that the image of u^t lies in $I^t(M/N)$ for all t, in which case we may write

$$u_t = v_t + w_t \in I^t M + N$$

for every t, where $v_t \in I^t M$ and $w_t \in N$. We claim that w_t is a Cauchy sequence in M that represents y. First, $w_t - w_{t+1} \in I^t M \cap N$ for all t. Since each $w_t \in N$, we see that the elements w_t form a Cauchy sequence in N by the Artin–Rees Theorem 10.4.2 since

$$w_t - w_{t+1} \in I^t M \cap N = I^{t-c}(I^c M \cap N) \subseteq I^{t-c} N$$

for all $t \geq c$. Thus, every element in $\ker(\widehat{M}^I \to \widehat{Q}^I)$ is in the image of $\widehat{N}^I$.

It remains to show that $0 \to \widehat{N}^I \to \widehat{M}^I$ is injective. Suppose $z_0, z_1, z_2, \ldots$ is a Cauchy sequence in N that converges to 0 in M. Then, z_t already converges to 0 in N, and this shows that $\widehat{N}^I$ injects into $\widehat{M}^I$.

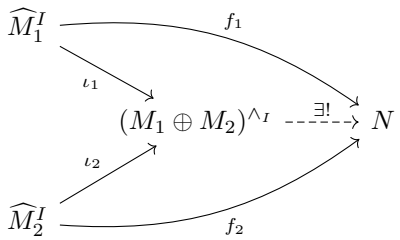
(*b*). Consider a presentation

$$R^{\oplus n} \xrightarrow{A} R^{\oplus m} \longrightarrow M \longrightarrow 0$$

for M, where $A = (r_{ij})$ is an $m \times n$ matrix with entries in R. We then have the commutative diagram

$$\begin{array}{ccccccc}
\widehat{R}^I \otimes_R R^{\oplus n} & \xrightarrow{\mathrm{id}\otimes A} & \widehat{R}^I \otimes_R R^{\oplus m} & \longrightarrow & \widehat{R}^I \otimes_R M & \longrightarrow & 0 \\
\downarrow{\scriptstyle \theta_{R^{\oplus n}}} & & \downarrow{\scriptstyle \theta_{R^{\oplus m}}} & & \downarrow{\scriptstyle \theta_M} & & \\
\widehat{R^{\oplus n}}^I & \xrightarrow{A} & \widehat{R^{\oplus m}}^I & \longrightarrow & \widehat{M}^I & \longrightarrow & 0
\end{array}$$

where the top row is exact by the right exactness of tensor products. The bottom row is exact by (*a*), where we think of the matrix A with terms in $\widehat{R}^I$ by applying the map $R \to \widehat{R}^I$ to each term in the matrix. The squares commute because θ is a natural transformation. The left vertical maps are isomorphisms because both tensor products and completions commute with finite direct sums: $(M_1 \oplus M_2)^{\wedge_I}$ satisfies the universal property for direct sums



where the dashed map is defined by mapping a Cauchy sequence $u_n \oplus v_n \in M_1 \oplus M_2$ to the Cauchy sequence $f_1(u_n) + f_2(u_n) \in N$. But then, θ_M is an isomorphism because cokernels of isomorphic maps are isomorphic.

(c). We need to show that $\widehat{R}^I \otimes_R N \to \widehat{R}^I \otimes_R M$ is injective for every pair of R-modules $N \subseteq M$. This holds for finitely generated N and M by (a) and (b). The result now follows from Theorem 10.4.6 below. Finally, the faithful flatness statement holds since the maximal ideal of R maps into the maximal ideal of $\widehat{R}^I$ by Proposition 10.3.6, and hence $R \to \widehat{R}^I$ is a flat local map of local rings. □

We did not prove the following theorem in class.

[AK21, (7.9)]

THEOREM 10.4.6 (Filtered direct limits are exact). *Let R be a ring and let I be a filtered partially ordered set. Let $\mathcal{C}$ be the category of 3-term exact sequences of R-modules: its objects are 3-term exact sequences, and its morphisms are commutative diagrams of the form*

$$\begin{array}{ccccc} L & \longrightarrow & M & \longrightarrow & N \\ \downarrow & & \downarrow & & \downarrow \\ L' & \longrightarrow & M' & \longrightarrow & N'. \end{array}$$

Then, for any filtered direct system

$$\{L_i \xrightarrow{\beta_i} M_i \xrightarrow{\gamma_i} N_i\}_{i \in I}$$

the induced sequence

$$\varinjlim_i L_i \xrightarrow{\beta} \varinjlim_i M_i \xrightarrow{\gamma} \varinjlim_i N_i$$

is exact.

Proof. Abusing notation, we denote by f_{ij} the transition maps connecting the L_i, M_i, or N_i, and by φ_i the canonical morphisms mapping the L_i, M_i, or N_i to their respective direct limits.

We first show that $\operatorname{im}(\beta) \subseteq \ker(\gamma)$. Suppose $\ell \in \operatorname{im}(\beta)$. By definition of direct limits (Example 10.2.5(2)), there exist $i \in I$ and $\ell_i \in L_i$ such that $\varphi_i(\ell_i) = \ell$. We then consider the commutative diagram

$$\begin{array}{ccccc} L_i & \xrightarrow{\beta_i} & M_i & \xrightarrow{\gamma_i} & N_i \\ {\scriptstyle\varphi_i}\downarrow & & \downarrow{\scriptstyle\varphi_i} & & \downarrow{\scriptstyle\varphi_i} \\ \varinjlim_i L_i & \xrightarrow{\beta} & \varinjlim_i M_i & \xrightarrow{\gamma} & \varinjlim_i N_i. \end{array} \tag{10.4.7}$$

Since $\operatorname{im}(\beta_i) \subseteq \ker(\gamma_i)$ by assumption, we see that

$$(\gamma \circ \beta)(\ell) = (\gamma \circ \beta)\big(\varphi_i(\ell_i)\big) = \varphi_i\big((\gamma_i \circ \beta_i)(\ell_i)\big) = 0.$$

We now show that $\operatorname{im}(\beta) \supseteq \ker(\gamma)$. Suppose $m \in \ker(\gamma)$. By construction of filtered direct limits (Example 10.2.5(2)), there exist $i \in I$ and $m_i \in M_i$ such that $\varphi_i(m_i) = m$ and hence $\varphi_i(\gamma_i(m_i)) = 0$ by the commutativity of (10.4.7). By construction of filtered direct limits (Example 10.2.5(2)), we know there exists $j \geq i$

such that $f_{ij}(m_i) = 0$. We now consider the commutative diagram

$$\begin{array}{ccccc}
L_i & \xrightarrow{\beta_i} & M_i & \xrightarrow{\gamma_i} & N_i \\
\downarrow{\scriptstyle f_{ij}} & & \downarrow{\scriptstyle f_{ij}} & & \downarrow{\scriptstyle f_{ij}} \\
L_j & \xrightarrow{\beta_j} & M_j & \xrightarrow{\gamma_j} & N_j \\
\downarrow{\scriptstyle \varphi_j} & & \downarrow{\scriptstyle \varphi_j} & & \downarrow{\scriptstyle \varphi_j} \\
\varinjlim_i L_i & \xrightarrow{\beta} & \varinjlim_i M_i & \xrightarrow{\gamma} & \varinjlim_i N_i.
\end{array}$$

By exactness in the j-th row, we know there exists $\ell_j \in L_j$ such that $\beta_j(\ell_j) = f_{ij}(m_i)$. Let $\ell = \varphi_j(\ell_j)$. By the commutativity of the diagram in the bottom two rows, we see that

$$\beta(\ell) = \beta\big(\varphi_j(\ell_j)\big) = \varphi_j\big(\beta_j(\ell_j)\big) = \varphi_j(m_j) = m. \qquad \square$$

We end our discussion of the Artin–Rees Theorem 10.4.2 with the following conjecture due to Craig Huneke, who was previously at Purdue (and served as head). Below, an *excellent ring* is a class of rings that is more restrictive than N-2, but still contains all fields, complete local rings, and localizations of finite type algebras over those rings. See [EGAIV$_2$, Définition 7.8.2] for the definition.

Conjecture 10.4.8 (Uniform Artin–Rees [Hun92, Conjecture 1.3]). *Let R be an excellent Noetherian ring of finite Krull dimension. Let $N \subseteq M$ be finitely generated R-modules. Then, there exists an integer $c = c(N, M)$ such that for* all *ideals $I \subseteq R$ and for all $n \geq c$, we have*

$$I^n M \cap N \subseteq I^{n-c} N.$$

In other words, Huneke's Conjecture 10.4.8 predicts that the integer c appearing in the Artin–Rees Theorem 10.4.2 only depends on N and M, and not on the ideal I. The special case where I runs over all maximal ideals in R was asked by Eisenbud and Hochster [EH79, Remark 3]. This special case was answered by Duncan and O'Carroll [OCa87, Theorem; DO89, Theorem; DO90, Remark]. O'Carroll also showed a similar uniform Artin–Rees statement where I runs over all principal ideals [OCa91, Theorem 1]. In general, Huneke's Uniform Artin–Rees Conjecture 10.4.8 is known in the following cases:

(1) R is a localization of a finite type algebra over an excellent Noetherian local ring [Hun92, Theorem 4.12(i)].
(2) R is of prime characteristic $p > 0$ and the Frobenius map $F\colon R \to R$ is module-finite [Hun92, Theorem 4.12(ii)].
(3) R is a localization of a finite type $\mathbf{Z}$-algebra [Hun92, Theorem 4.12(iii)].
(4) R is an excellent Noetherian domain of dimension ≤ 3 [Hun92, Proposition 5.1, Theorems 5.3 and 5.11].
(5) R is an excellent Noetherian $\mathbf{Q}$-algebra that is a quotient of a regular ring of finite Krull dimension ([Hun00, Theorem 5.4] plus [Tem08, Theorem 1.1]).

10.5. Further applications of completions

I want to end with some pointers for why completions are important, and where commutative algebra goes from here.

10.5.1. Algebraic number theory. In algebraic number theory, you introduce the p-adic integers to give some analytic tools for (for example) finding solutions to Diophantine equations after reducing modulo p. This a special case of the following:

[AM69, Exer. 10.9]
[Hoc20, p. 3]

LEMMA 10.5.1 (Hensel's lemma). *Let $(A, \mathfrak{m})$ be a local ring that is $\mathfrak{m}$-adically complete. For any polynomial $f(x) \in A[x]$, denote by $\bar{f}(x) \in (A/\mathfrak{m})[x]$ the polynomial obtained by reducing its coefficients modulo $\mathfrak{m}$. If $f(x)$ is monic of degree n and if there exist coprime monic polynomials*

$$\bar{g}(x), \bar{h}(x) \in (A/\mathfrak{m})[x]$$

of degrees $r, n-r$ with

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x),$$

then we can lift $\bar{g}(x), \bar{h}(x)$ back to monic polynomials $g(x), h(x) \in A[x]$ such that

$$f(x) = g(x)h(x).$$

The proof follows pretty much by building formal power series in A for the coefficients one step at a time. Setting $A = \hat{\mathbf{Z}}_7$ (the ring of 7-adic integers), since $x^2 - 2$ has a root $3 \in \hat{\mathbf{Z}}_7/(y) \cong \mathbf{Z}/(7)$, we see that 2 is a square in $\hat{\mathbf{Z}}_7$. You can also use this to study the equation

$$z^2 - (1 + x)$$

from before to produce a square-root for $1 + x$, even without Taylor series. Hensel's lemma is connected to the implicit function theorem in calculus, since it allows you to solve implicit functions.

10.5.2. Algebraic geometry. In algebraic geometry, we have already seen how completions give "more local" data that cannot be detected after just localizing. Over the complex numbers, this reflects the fact that the Zariski topology is much coarser than the topology you would get by considering a complex algebraic variety as a complex manifold. This is why Serre introduced flatness to begin with in [GAGA, §21]. If

$$X = \{f_1 = f_2 = \cdots = f_n = 0\} \subseteq \mathbf{C}^n$$

is a complex algebraic variety of dimension d all of whose local rings are regular local rings, then one can consider the local ring $\mathcal{O}_x$ obtained by localizing the coordinate ring $A(X)$ of X at a maximal ideal $\mathfrak{m}_x \subseteq R$, or the local ring $\mathcal{H}_x$ obtained by considering X as a complex manifold and looking at germs of holomorphic functions of X at x. Serre showed that both rings $\mathcal{O}_x$ and $\mathcal{H}_x$ have the same completion

$$\mathbf{C}[\![x_1, x_2, \ldots, x_d]\!]$$

in [GAGA, Proposition 4, Corollaire 1]. This enabled him to prove that algebraic geometry and analytic geometry are very closely related. Since both $\mathcal{O}_x$ and $\mathcal{H}_x$ are Noetherian, the maps are faithfully flat, which provide a means to move back and forth between the algebraic and analytic contexts. For example, dimensions are preserved [GAGA, Proposition 4, Corollaire 2]. A particularly important application of Serre's results is that a complex analytic space that is locally defined as the vanishing set of holomorphic equations in $\mathbf{P}^n_{\mathbf{C}}$ is in fact algebraic in [GAGA, Proposition 13]. This is known as Chow's theorem, and was previously shown by Chow using analytic methods [Cho49, Theorem V].

10.5.3. Commutative algebra. In commutative algebra, we have already seen that finitely generated algebras over fields are particularly nice: We have Noether's normalization theorem, a simple proof of Hilbert's basis theorem, and used some of these ideas to build up a nice theory of dimension for these rings and to prove that these rings are N-2. While these rings encompass the ones usually seen in algebraic geometry, not all rings are of this form.

On the other hand, for every Noetherian ring there is a procedure to reduce problems to the complete local case: you first localize at a prime ideal, and then take the completion at the expansion of that prime ideal. The rings you end up with are very nice, and have the following analogue of Noether normalization:

THEOREM 10.5.2 (Cohen's structure theorem [Coh46]). *Let $(A, \mathfrak{m})$ be a local Noetherian ring that is $\mathfrak{m}$-adically complete. Then, it is a quotient of a regular local ring. If A contains a field, then there exists a field $k \subseteq A$ such that* [Hoc20]

$$k[\![x_1, x_2, \dots, x_n]\!] \twoheadrightarrow A.$$

Moreover, A is module-finite over a formal power series ring

$$k[\![x_1, x_2, \dots, x_d]\!] \subseteq A.$$

If A does not contain a field, then there exists a complete DVR $A_0 \subseteq A$ such that

$$A_0[\![x_2, x_3, \dots, x_n]\!] \twoheadrightarrow A.$$

Moreover, if A is a domain, then A is module-finite over a formal power series ring

$$A_0[\![x_2, x_3, \dots, x_d]\!] \subseteq A.$$

Using this, one can show that complete local Noetherian domains containing fields are N-2, mimicking the proof from before.

Cohen's structure theorem is a very important theorem in modern commutative algebra. Proofs of major results often go by first reducing to the complete local case by localizing then completing (which is a composition of flat maps, hence flat itself), and then using Cohen's structure theorem to reduce the question to something more explicit using power series rings.

Index

Page numbers in bold refer to definitions. An "f", "n", or "t" following a page number refers to a figure, footnote, or table on that page, respectively.

Abhyankar, Shreeham S., 3, 45
Abhyankar–Moh–Suzuki theorem, **3**
algebra, **31**
  finitely generated, **31**
  module-finite, **32**
algebraic set $Z(I)$, **65**
annihilator
  of an element, $\mathrm{Ann}_R(m)$, **25**
  of an module, $\mathrm{Ann}_R(M)$, **25**
Artin, Emil, 81, 85, 183
  –Rees lemma, *see* Artin–Rees lemma
Artin, Michael, 10
Artin–Rees lemma, 183, **183**
ascending chain condition (ACC), **81**
assassin, *see* associated prime
associated prime, **130**
Azumaya, Goro, 26

Bhatwadekar, S. M., 46
bilinear map, **101**
Brownawell, W. Dale, 73

category, **19**
  opposite, **19**
Cauchy, Augustin-Louis
  sequence for the I-adic topology, **177**
Cayley–Hamilton theorem, 47
chain
  saturated, of prime ideals, **73**
Chen, Huayi, 73
Chow, Wei-Liang, 188
  theorem, 188
Claborn, Luther, 163
cofiltered
  inverse limit, **177**
  inverse system, **177**
Cohen, Irvin S., 45, 52
  structure theorem, **189**
Cohen–Macaulay ring or module, **150**
Cohen–Seidenberg theorems, 52–56, 60–63
coimage, **26**
cokernel, **26**
contraction of an ideal, **5**
coordinate function x_i, **93**
coordinate ring $k[X]$, **93**
coproduct, **23**
cuspidal cubic, 66f
cuspidal cubic curve, 51

dévissage, **133**
Danielewski, Wlodzimierz, 45
degree $\deg(f)$, **2**
depth, **148**
descending chain condition (DCC), **81**
determinant trick, **47**
determinantal
  ring, 91
  variety, 91
dimension
  of a module, **145**
dimension formula, **78**
  counterexample, **78**
direct
  limit, **174**
  system, **174**
division algorithm, **60**
divisor, **160**

class group Cl(R), **161**
principal, **160**
domain, **9**
Duncan, Andrew J., 187
DVR (discrete rank one valuation domain), **76**

Eakin, Paul, 45
Eisenbud, David, 187
Eisenbud–Mazur conjecture, **164**
element
algebraically independent, **67**
identity, **1**
zero, **1**
equivalence
anti- of categories, **22**
of categories, **22**
espace étalé, 40
exact sequence, **29**
short, **29**
split, **29**
excellent ring, 187
extension of an ideal, **5**

fiber, **56**
field, **2**
fraction, **35**
residue, **27**, 38
filtered
direct limit, **174**
exactness of, 186
direct system, **174**
union, **174**
filtration
factors of, 132
finite ascending, **132**
length of, **132**
prime cyclic, **133**
finite type
algebra, **47**
map, **47**
Fujita, Takao, 46
functor, **20**
contravariant, **20**
covariant, **20**
representable, **22**
functor of points, 96

Gabber, Ofer, 73
going down, **60**
going up, **54**
group action, **97**
Gunning, Robert C., 150
Gupta, Neena, 46

Hartogs, Friedrich
algebraic – lemma, **164**
Hartshorne, Robin, 17, 150
conjecture, 17
Heinrich, Katharina, 73
Heinzer, William, 45
Hensel, Kurt
lemma, **188**
Hermann, Grete, 72
Hilbert, David, 1
basis theorem, **85**, 85–86
for formal power series, **98**
over fields, **85**
Nullstellensatz, **70**, 69–73
effective, **73**
geometric version, **65**
weak forms, 69–70
Hochster, Melvin, 10, 43, 45, 187
Huneke, Craig, 187

I-adic completion, **178**
I-adically complete, **178**
I-adically separated, **178**
ideal, **4**
generated by, **4**
indecomposable, **128**
intersection of, **4**
irreducible, **128**
maximal, **10**
of a subset of $\mathbf{A}^n_k$, 88
primary, **125**
prime, **9**
associated, *see* associated prime
principal, **4**
product of, **4**
proper, **4**
radical of, $\sqrt{I}$, **8**
sum of, **4**
incomparability, **53**
insertion morphisms, **174**
integers $\mathbf{Z}$, **2**
integral
algebra, **47**

closure, **50**
element, **46**
extension, **47**
map, **47**
integral closure
of rings, **49**
localizes, **51**
integrally closed domain, **50**
inverse
limit, **177**
system, **176**
irreducible
component, **90**
decomposition, **90**
topological space, *see* topological space, irreducible
isomorphism, **19**
of functors, **21**
of rings, **2**

Jacobian
conjecture, **4**
determinant, **4**
Jacobson, Nathan, 27
ring, 93
Japanese ring, **165**

Keller, Ott-Heinrich, 4
kernel
of a ring map, **5**
Kollár, János, 73
Krull dimension, $\dim(R)$, **45**
Krull, Wolfgang, 26, 45, 52, 141, 158
criterion for normality, **158**
height theorem, **142**
intersection theorem, 137
principal ideal theorem, **141**
Kuratowski, Kazimierz, 11
–Zorn lemma, *see* Kuratowski–Zorn lemma
Kuratowski–Zorn lemma, **11**

Lasker, Emanuel, 125
law
distributive, **5**
modular, **5**
Leedham-Green, Charles R., 163
length, **138**
finite, **138**
local cohomology, 87
localization
of modules, **38**
of rings, **32**
lying over, **52**

Mac Lane, Saunders, 59
Macaulay, Francis S.
curve, **150**
map
projection, **23**
Masser, David W., 72
Mazur, Barry
Eisenbud–Mazur conjecture, **164**
Miyanishi, Masayoshi, 46
module, **23**
Artinian, **81**
cyclic, **133**
finitely presented, **108**
Noetherian, **81**
presentation of, **108**
finite, **108**
prime cyclic, **133**
quotient, **26**
simple, **138**
sub, **24**
torsion, $T(M)$, **25**
torsion-free, **25**
module-finite
algebra, **47**
extension, **47**
map, **47**
Moh, Tzuong Tsieng, 3
morphism
of algebraic sets, **93**

N-1, **165**
N-2, **165**
Nagata, Masayoshi, 183
altitude formula, 78
Nakayama, Tadashi
lemma, **26**
natural transformation, **21**
Noether, Emmy, 1, 4, 45, 81, 97, 125
isomorphism theorems, **26**
normalization theorem, **67**, 65–69
geometric version, **65**
nonzerodivisor (nzd), **33**
normal, **159**

domain, **50**
is a local property for domains, 51
normal closure, **168**
normalization, **50**
localizes, **51**

O'Carroll, Liam, 187
object of a category, **19**

p-adic integers $\mathbf{Z}_p$, **82**
partially ordered set
filtered or directed, **173**
point
generic, 14, **42**
primary decomposition, **126**
irredundant, **127**
product, **23**
property
local, **39**
pure transcendental extension, **75**

Rabinowitsch, J.L.
trick, *see* Rainich, George Yuri, trick
Rainich, George Yuri
trick, 70
reducible
topological space, *see* topological space, reducible
reducible set or space
empty set as example of, 42
Rees, David, 183
algebra, **183**
Artin– lemma, *see* Artin–Rees lemma
regular map, **93**
regular sequence, **146**
improper, **146**
represents, *see* functor, representable
restriction of scalars, **37**
resultant, 50
ring, **1**
biequidimensional, **73**
catenary, **78**
commutative, **1**
equicodimensional, **73**
counterexample, 77
formal power series, **28**
generated by, **2**
map, **2**
of algebraic integers, 50
of invariants, **97**
polynomial, **2**
reduced, **8**
is a local property, **39**
total quotient, **35**
zero, **1**
ring of fractions, *see* localization of rings
Rosen, Michael, 163
Russell, Peter, 46

Samuel, Pierre, 150
scheme, 92
Seidenberg, Abraham, 45, 52
sequence
Cauchy, *see* Cauchy sequence
null, **178**
Serre, Jean-Pierre, 159, 188
condition (S_k), **150**
criterion for normality, **159**
set
closed, **13**
difference $A - B$, **xi**
multiplicative, **9**, 32
open, **13**
principal, $D(f)$, **14**
Sharp, Rodney Y., 183
Shiffman, Bernard, 72
snake lemma, **29**
Sombra, Martín, 73
spectrum, $\operatorname{Spec}(R)$, **10**
maximal, $\operatorname{MaxSpec}(R)$, **10**
quasi-compactness of, 41
subring, **2**
Sugie, Tohru, 46
Suzuki, Masakazu, 3
system of parameters, **143**
for a module, **146**

Tate, John, 85
tensor product, $M \otimes_R N$, **101**, 101–104
is not exact, 105
is right exact, 104
Thompson, Mary L., 10, 72
Tietze, Heinrich Franz Friedrich
extension theorem, 93

topological space, **13**
  irreducible, **42**
  Noetherian, 90
  quasi-compact, **41**
  quasi-separated, 42
  reducible, **42**
  sober, **42**
  spectral, 43
topology, **13**
transcendence
  basis, **75**
  degree, $\mathrm{trdeg}_k(K)$, **76**
twisted cubic curve, 10, 28, 36

UFD
  is normal, **50**
universal property
  localization of modules, **175**
  localization of rings, **32**
  quotient rings, **6**

variety
  affine, **90**

Wüstholz, Gisbert, 72
Weber, Heinrich, 1

Yoneda, Nobuo, 59
  lemma, **59**

Zariski, Oscar
  Nullstellensatz, **68**
  topology, **13**
  topology on k^n, 70
zerodivisor, **33**
Zorn, Max, 11
  lemma, *see* Kuratowski–Zorn lemma

Bibliography

[AEH72] Shreeram S. Abhyankar, Paul Eakin, and William Heinzer. "On the uniqueness of the coefficient ring in a polynomial ring." *J. Algebra* 23 (1972), pp. 310–342. DOI: 10.1016/0021-8693(72)90134-2. MR: 306173. 45

[AK21] Allen B. Altman and Steven L. Kleiman. *A term of commutative algebra*. Version on ResearchGate. Cambridge, MA: Worldwide Center of Mathematics, 2021. DOI: 10.13140/RG.2.2.31866.62400. xi, xiii, 1, 2, 4–17, 19, 20, 23–29, 31, 33–39, 43, 45–55, 57, 60, 67, 68, 70–74, 76–78, 81–86, 101–114, 117–119, 126–128, 138, 141–143, 157–159, 163–168, 174, 175, 186

[Aki35] Yasuo Akizuki. "Teilerkettensatz und Vielfachenkettensatz." *Proc. Phys.-Math. Soc. Japan (3)* 17 (1935), pp. 337–345. DOI: 10.11429/ppmsj1919.17.0_337. ZBL: 0012.24502. 140

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Reading, MA: Addison-Wesley Publishing Co., 1969. DOI: 10.1201/9780429493638. MR: 242802. xi, xiii, 1, 2, 4, 5, 7, 9, 29, 34, 35, 39, 47, 51, 52, 67, 68, 81–84, 86, 98, 101, 102, 104–108, 110, 117, 118, 121, 125–129, 141–143, 178, 188

[AM75] Shreeram S. Abhyankar and Tzuong Tsieng Moh. "Embeddings of the line in the plane." *J. Reine Angew. Math.* 276 (1975), pp. 148–166. DOI: 10.1515/crll.1975.276.148. MR: 379502. 3

[And18] Yves André. "La conjecture du facteur direct." *Publ. Math. Inst. Hautes Études Sci.* 127 (2018), pp. 71–93. DOI: 10.1007/s10240-017-0097-9. MR: 3814651. 166

[Azu51] Gorô Azumaya. "On maximally central algebras." *Nagoya Math. J.* 2 (1951), pp. 119–150. DOI: 10.1017/S0027763000010114. MR: 40287. 26

[BG15] S. M. Bhatwadekar and Neena Gupta. "A note on the cancellation property of $k[X, Y]$." *J. Algebra Appl.* 14.9 (2015), 1540007, 5 pp. DOI: 10.1142/S0219498815400071. MR: 3368259. 46

[BH98] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*. Revised edition. Cambridge Stud. Adv. Math., Vol. 39. Cambridge: Cambridge Univ. Press, 1998. DOI: 10.1017/CBO9780511608681. MR: 1251956. 154

[BouCA] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Translated from the French. Paris: Hermann; Reading, MA: Addison-Wesley Publishing Co., 1972. ark:/13960/t56f3ng94. MR: 360549. 1, 42, 134, 137

[BouGT] Nicolas Bourbaki. *General topology. Chapters 1–4*. Translated from the French, Reprint of the 1989 English translation. Elem. Math. (Berlin). Berlin: Springer-Verlag, 1998. DOI: 10.1007/978-3-642-61701-0. MR: 1726779. 41

[Bro87] W. Dale Brownawell. "Bounds for the degrees in the Nullstellensatz." *Ann. of Math. (2)* 126.3 (1987), pp. 577–591. DOI: 10.2307/1971361. MR: 916719. 73

[BV88] Winfried Bruns and Udo Vetter. *Determinantal rings*. Lecture Notes in Math., Vol. 1327. Berlin: Springer-Verlag, 1988. DOI: 10.1007/BFb0080378. MR: 953963. 91

[Cho49] Wei-Liang Chow. "On compact complex analytic varieties." *Amer. J. Math.* 71 (1949), pp. 893–914. DOI: 10.2307/2372375. MR: 33093. 188

[Cla66] Luther Claborn. "Every abelian group is a class group." *Pacific J. Math.* 18 (1966), pp. 219–222. DOI: 10.2140/pjm.1966.18.219. MR: 195889. 163

[Coh46] Irvin S. Cohen. "On the structure and ideal theory of complete local rings." *Trans. Amer. Math. Soc.* 59 (1946), pp. 54–106. DOI: 10.2307/1990313. MR: 16094. 189

[Cor00] Leo Corry. "The origins of the definition of abstract rings." *Mod. Log.* 8.1-2 (2000), pp. 5–27. URL: https://projecteuclid.org/euclid.rml/1081878062. MR: 1834715. 1

[Cor04] ———. *Modern algebra and the rise of mathematical structures*. Second ed. Basel: Birkhäuser Verlag, 2004. DOI: 10.1007/978-3-0348-7917-0. MR: 2033171. 1

[CS46] Irvin S. Cohen and Abraham Seidenberg. "Prime ideals and integral dependence." *Bull. Amer. Math. Soc.* 52 (1946), pp. 252–261. DOI: 10.1090/S0002-9904-1946-08552-3. MR: 15379. 45, 52, 53, 55, 60

[Dan89] Wlodzimierz Danielewski. "On a cancellation problem and automorphism group of affine algebraic varieties." Preprint, Institute of Computer Science of Polish Academy of Sciences, Warsaw. 1989. 45

[Des66] Wilbur E. Deskins. *Abstract algebra*. New York: The Macmillan Co., New York; London: Collier-Macmillan Ltd., 1966. MR: 199066. 45

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third ed. Hoboken, NJ: John Wiley & Sons, Inc., 2004. MR: 2286236. 75, 169, 170

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Avec un appendice *Corps de classes local* par Michiel Hazewinkel. Paris: Masson & Cie, Éditeurs; Amsterdam: North-Holland Publishing Co., 1970. MR: 302656. 96

[DO89] Andrew J. Duncan and Liam O'Carroll. "A full uniform Artin-Rees theorem." *J. Reine Angew. Math.* 394 (1989), pp. 203–207. DOI: 10.1515/crll.1989.394.203. MR: 977443. 187

[DO90] ———. "On Zariski-regularity, the vanishing of Tor and a uniform Artin-Rees theorem." *Topics in algebra, Part 2 (Warsaw, 1988)*. Banach Center Publ., Vol. 26, Part 2. PWN, Warsaw, 1990, pp. 49–55. URL: https://bibliotekanauki.pl/articles/720027. MR: 1171259. 187

[Edw80] Harold M. Edwards. "The genesis of ideal theory." *Arch. Hist. Exact Sci.* 23.4 (1980), pp. 321–378. DOI: 10.1007/BF00327914. MR: 608312. 4

[EGAI] Alexander Grothendieck and Jean A. Dieudonné. "Éléments de géométrie algébrique. I. Le langage des schémas." *Inst. Hautes Études Sci. Publ. Math.* 4 (1960), 228 pp. NUMDAM: PMIHES_1960__4__5_0. DOI: 10.1007/BF02684778. MR: 217083. 175

[EGAI$_{\text{new}}$] ———. *Eléments de géométrie algébrique. I.* Grundlehren Math. Wiss., Vol. 166. Berlin: Springer-Verlag, 1971. ark:/13960/t42s6kw4b. MR: 3075000. 42, 93, 175

[EGAIV$_1$] ———. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I." *Inst. Hautes Études Sci. Publ. Math.* 20 (1964), 259 pp. NUMDAM: PMIHES_1964__20__5_0. DOI: 10.1007/BF02684747. MR: 173675. 42, 73, 78, 165

[EGAIV$_2$] ———. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II." *Inst. Hautes Études Sci. Publ. Math.* 24 (1965), 231 pp. NUMDAM: PMIHES_1965__24__5_0. DOI: 10.1007/BF02684322. MR: 199181. 150, 159, 187

[EH79] David Eisenbud and Melvin Hochster. "A Nullstellensatz with nilpotents and Zariski's main lemma on holomorphic functions." *J. Algebra* 58.1 (1979), pp. 157–161. DOI: 10.1016/0021-8693(79)90196-0. MR: 535850. 187

[EM97] David Eisenbud and Barry Mazur. "Evolutions, symbolic squares, and Fitting ideals." *J. Reine Angew. Math.* 488 (1997), pp. 189–201. DOI: 10.1515/crll.1997.488.189. MR: 1465370. 164

[Fuj79] Takao Fujita. "On Zariski problem." *Proc. Japan Acad. Ser. A Math. Sci.* 55.3 (1979), pp. 106–110. DOI: 10.3792/pjaa.55.106. MR: 531454. 46

[GAGA] Jean-Pierre Serre. "Géométrie algébrique et géométrie analytique." *Ann. Inst. Fourier (Grenoble)* 6 (1956), pp. 1–42. DOI: 10.5802/aif.59. MR: 82175. 105, 188

[Ger61] Murray Gerstenhaber. "On dominance and varieties of commuting matrices." *Ann. of Math. (2)* 73 (1961), pp. 324–348. DOI: 10.2307/1970336. MR: 132079. 10

[God73] Roger Godement. *Topologie algébrique et théorie des faisceaux.* Troisième édition revue et corrigée. Actualités Sci. Indust., Vol. 1252. Publications de l'Institut de Mathématique de l'Université de Strasbourg, Vol. XIII. Paris: Hermann, 1973. MR: 345092. 40

[Gro95] Alexander Grothendieck. "Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules." *Séminaire Bourbaki, Vol. 5.* Paris: Soc. Math. France, 1995, Exposé No. 195, pp. 369–390. NUMDAM: SB_1958-1960__5__369_0. MR: 1603480. 59

[Gup14a] Neena Gupta. "On the cancellation problem for the affine space $\mathbb{A}^3$ in characteristic p." *Invent. Math.* 195.1 (2014), pp. 279–288. DOI: 10.1007/s00222-013-0455-2. MR: 3148104. 46

[Gup14b] Neena Gupta. "On Zariski's cancellation problem in positive characteristic." *Adv. Math.* 264 (2014), pp. 296–307. DOI: 10.1016/j.aim.2014.07.012. MR: 3250286. 46

[Har62] Robin Hartshorne. "Complete intersections and connectedness." *Amer. J. Math.* 84.3 (1962), pp. 497–508. DOI: 10.2307/2372986. MR: 142547. 150

[Har70] ———. *Ample subvarieties of algebraic varieties*. Notes written in collaboration with C. Musili. Lecture Notes in Math., Vol. 156. Berlin-New York: Springer-Verlag, 1970. DOI: 10.1007/BFb0067839. MR: 282977. 17

[Har77] ———. *Algebraic geometry*. Grad. Texts in Math., Vol. 52. New York-Heidelberg: Springer-Verlag, 1977. DOI: 10.1007/978-1-4757-3849-0. MR: 463157. 17, 40, 42, 78, 82, 88, 92, 93, 120, 163

[Har79] ———. "Complete intersections in characteristic $p > 0$." *Amer. J. Math.* 101.2 (1979), pp. 380–383. DOI: 10.2307/2373984. MR: 527998. 18

[HE71] Melvin Hochster and John A. Eagon. "Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci." *Amer. J. Math.* 93 (1971), pp. 1020–1058. DOI: 10.2307/2373744. MR: 302643. 151

[Hei02] Raymond C. Heitmann. "The direct summand conjecture in dimension three." *Ann. of Math. (2)* 156.2 (2002), pp. 695–712. DOI: 10.2307/3597204. MR: 1933722. 166

[Hei17] Katharina Heinrich. "Some remarks on biequidimensionality of topological spaces and Noetherian schemes." *J. Commut. Algebra* 9.1 (2017), pp. 49–63. DOI: 10.1216/JCA-2017-9-1-49. MR: 3631826. 73, 78

[Her26] Grete Hermann. "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale." *Math. Ann.* 95.1 (1926), pp. 736–788. DOI: 10.1007/BF01206635. MR: 1512302. 72

[Her75] I. N. Herstein. *Topics in algebra*. Second edition. Lexington, Mass.-Toronto, Ont.: Xerox College Publishing, 1975. ark:/13960/t3d01rw9t. MR: 356988. 50

[Hil1890] David Hilbert. "Ueber die Theorie der algebraischen Formen." *Math. Ann.* 36.4 (1890), pp. 473–534. DOI: 10.1007/BF01208503. MR: 1510634. 85

[Hil1893] ———. "Ueber die vollen Invariantensysteme." *Math. Ann.* 42.3 (1893), pp. 313–373. DOI: 10.1007/BF01444162. MR: 1510781. 70

[Hil1897] ———. "Die Theorie der algebraischen Zahlkörper." *Jahresber. Deutsch. Math.-Verein.* 4 (1897), pp. i–xviii + 175–546. URL: http://eudml.org/doc/144518. ZBL: 28.0157.05. 1

[HK71] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second edition. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1971. ark:/13960/s275jtrgzgt. MR: 276251. 47

[Hoc07] Melvin Hochster. *Foundations of tight closure theory*. Lecture notes from a course taught at the University of Michigan, Fall 2007. URL: https://dept.math.lsa.umich.edu/~hochster/711F07/fndtc.pdf. 27

[Hoc16a] ———. *Depth, Cohen-Macaulay rings, and flatness*. Supplementary material from a course taught at the University of Michigan, Winter

2016. URL: https://dept.math.lsa.umich.edu/~hochster/615W16/615supp.pdf. 148, 150

[Hoc16b] ———. *Math 615 lecture notes*. Lecture notes from a course taught at the University of Michigan, Winter 2016. URL: https://dept.math.lsa.umich.edu/~hochster/615W16/615W16.pdf. 145–150, 152, 154

[Hoc17] ———. *Math 614 lecture notes*. Lecture notes from a course taught at the University of Michigan, Fall 2017. URL: https://dept.math.lsa.umich.edu/~hochster/614F17/614.pdf. xi, xiii, 1, 2, 9, 10, 19–22, 24, 27, 31–35, 37, 39, 41–43, 45–63, 65–71, 73–77, 81–86, 88–91, 93, 94, 96, 98, 101, 102, 104–108, 110–114, 117, 118, 120–123, 125–146, 157–161, 163–167, 169, 171, 173, 174, 176–184

[Hoc20] ———. "The structure theory of complete local rings." Supplementary notes from a course taught at the University of Michigan, Winter 2020. URL: http://www.math.lsa.umich.edu/~hochster/615W20/supStructure.pdf. 188, 189

[Hoc20a] ———. *Math 614 lecture notes*. Lecture notes from a course taught at the University of Michigan, Fall 2020. URL: https://dept.math.lsa.umich.edu/~hochster/614F20/614Lx.pdf. 97

[Hoc20b] ———. *Topics in commutative algebra: Regular rings, Cohen-Macaulay rings and modules, multiplicities, and tight closure*. Lecture notes from a course taught at the University of Michigan, Winter 2020. URL: https://dept.math.lsa.umich.edu/~hochster/615W20/615W20.pdf. 148

[Hoc69] ———. "Prime ideal structure in commutative rings." *Trans. Amer. Math. Soc.* 142 (1969), pp. 43–60. DOI: 10.2307/1995344. MR: 251026. 43

[Hoc72a] ———. "Nonuniqueness of coefficient rings in a polynomial ring." *Proc. Amer. Math. Soc.* 34 (1972), pp. 81–82. DOI: 10.2307/2037901. MR: 294325. 45, 97

[Hoc72b] ———. "Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes." *Ann. of Math. (2)* 96 (1972), pp. 318–337. DOI: 10.2307/1970791. MR: 304376. 151

[Hoc73a] ———. "Contracted ideals from integral extensions of regular rings." *Nagoya Math. J.* 51 (1973), pp. 25–43. URL: http://projecteuclid.org/euclid.nmj/1118794784. MR: 349656. 166

[Hoc73b] ———. "Grassmannians and their Schubert subvarieties are arithmetically Cohen-Macaulay." *J. Algebra* 25 (1973), pp. 40–57. DOI: 10.1016/0021-8693(73)90074-4. MR: 314833. 151

[Hoc78] ———. "Some applications of the Frobenius in characteristic 0." *Bull. Amer. Math. Soc.* 84.5 (1978), pp. 886–912. DOI: 10.1090/S0002-9904-1978-14531-5. MR: 485848. 151

[HR74] Melvin Hochster and Joel L. Roberts. "Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay." *Advances in Math.* 13 (1974), pp. 115–175. DOI: 10.1016/0001-8708(74)90067-X. MR: 347810. 151

[Hun00] Craig Huneke. "Desingularizations and the uniform Artin-Rees theorem." *J. London Math. Soc. (2)* 62.3 (2000), pp. 740–756. DOI: 10.1112/S002461070000154X. MR: 1794281. 187

[Hun92] Craig Huneke. "Uniform bounds in Noetherian rings." *Invent. Math.* 107.1 (1992), pp. 203–223. DOI: 10.1007/BF01231887. MR: 1135470. 187

[ILO14] Luc Illusie, Yves Laszlo, and Fabrice Orgogozo, eds. *Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents*. Séminaire à l'École Polytechnique 2006–2008. With the collaboration of Frédéric Déglise, Alban Moreau, Vincent Pilloni, Michel Raynaud, Joël Riou, Benoît Stroh, Michael Temkin, and Weizhe Zheng. Astérisque, Vol. 363-364. Paris: Soc. Math. France, 2014. Corrected version available at http://fabrice.orgogozo.perso.math.cnrs.fr/travaux_de_Gabber/. MR: 3309086. 73

[Jac45] Nathan Jacobson. "The radical and semi-simplicity for arbitrary rings." *Amer. J. Math.* 67 (1945), pp. 300–320. DOI: 10.2307/2371731. MR: 12271. 27

[Jac85] _____. *Basic algebra. I.* Second edition. New York: W. H. Freeman and Company, 1985. MR: 780184. 50

[Jac89] _____. *Basic algebra. II.* Second edition. New York: W. H. Freeman and Company, 1989. Republication by Dover available at ark:/13960/s2jfr8f69g9. MR: 1009787. 168

[Kad18] Zhibek Kadyrsizova. "Nearly commuting matrices." *J. Algebra* 497 (2018), pp. 199–218. DOI: 10.1016/j.jalgebra.2017.10.019. MR: 3743180. 10

[Kel39] Ott-Heinrich Keller. "Ganze Cremona-Transformationen." *Monatsh. Math. Phys.* 47.1 (1939), pp. 299–306. DOI: 10.1007/BF01695502. MR: 1550818. 4

[Kin98] Yoshiki Kinoshita. "Nobuo Yoneda (1930–1996)." *Math. Japon.* 47.1 (1998), p. 155. MR: 1606356. 59

[Kol88] János Kollár. "Sharp effective Nullstellensatz." *J. Amer. Math. Soc.* 1.4 (1988), pp. 963–975. DOI: 10.2307/1990996. MR: 944576. 73

[KR00] Kazuhiko Kurano and Paul C. Roberts. "The positivity of intersection multiplicities and symbolic powers of prime ideals." *Compositio Math.* 122.2 (2000), pp. 165–182. DOI: 10.1023/A:1001741230307. MR: 1775417. 164

[Kru32] Wolfgang Krull. "Allgemeine Bewertungstheorie." *J. Reine Angew. Math.* 167 (1932), pp. 160–196. DOI: 10.1515/crll.1932.167.160. MR: 1581334. 158

[Kru36] _____. "Beiträge zur Arithmetik kommutativer Integritätsbereiche." *Math. Z.* 41.1 (1936), pp. 545–577. DOI: 10.1007/BF01180441. MR: 1545640. 52

[Kru37] _____. "Beiträge zur Arithmetik kommutativer Integritätsbereiche. III. Zum Dimensionsbegriff der Idealtheorie." *Math. Z.* 42.1 (1937), pp. 745–766. DOI: 10.1007/BF01160110. MR: 1545707. 45, 52

[Kru38] _____. "Dimensionstheorie in Stellenringen." *J. Reine Angew. Math.* 179 (1938), pp. 204–226. DOI: 10.1515/crll.1938.179.204. MR: 1581594. 141, 142

[Kur1922] Casimir Kuratowski. "Une méthode d'élimination des nombres transfinis des raisonnements mathématiques." *Fundamenta Mathematicae* 3

(1922), pp. 76–108. DOI: 10.4064/fm-3-1-76-108. ZBL: 48.0205.04. 11

[Lak72] Dan Laksov. "The arithmetic Cohen-Macaulay character of Schubert schemes." *Acta Math.* 129.1-2 (1972), pp. 1–9. DOI: 10.1007/BF02392211. MR: 382297. 151

[Lan02] Serge Lang. *Algebra*. Third edition. Grad. Texts in Math., Vol. 211. New York: Springer-Verlag, 2002. DOI: 10.1007/978-1-4613-0041-0. MR: 1878556. 75, 174

[Las1905] Emanuel Lasker. "Zur Theorie der moduln und Ideale." *Math. Ann.* 60.1 (1905), pp. 20–116. DOI: 10.1007/BF01447495. MR: 1511288. 125

[LG72] Charles R. Leedham-Green. "The class group of Dedekind domains." *Trans. Amer. Math. Soc.* 163 (1972), pp. 493–500. DOI: 10.2307/1995734. MR: 292806. 163

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*. Oxf. Grad. Texts Math., Vol. 6. Translated from the French by Reinie Erné. Oxford: Oxford Univ. Press, 2002. DOI: 10.1093/oso/9780198502845.001.0001. MR: 1917232. 119

[Lyu89] Gennady Lyubeznik. "A survey of problems and results on the number of defining equations." *Commutative algebra (Berkeley, CA, 1987)*. Math. Sci. Res. Inst. Publ., Vol. 15. New York: Springer, 1989, pp. 375–390. DOI: 10.1007/978-1-4612-3660-3_20. MR: 1015529. 17

[Mac94] Francis S. Macaulay. *The algebraic theory of modular systems*. Revised reprint of the 1916 original, With an introduction by Paul Roberts. Cambridge Math. Lib. Cambridge: Cambridge Univ. Press, 1994. Original 1916 edition available at ark:/13960/t2d79897m. MR: 1281612. 150

[Mac98] Saunders Mac Lane. "The Yoneda lemma." *Math. Japon.* 47.1 (1998), p. 156. MR: 1606360. 59

[Mar01] Thomas Marley. "The associated primes of local cohomology modules over rings of small dimension." *Manuscripta Math.* 104.4 (2001), pp. 519–525. DOI: 10.1007/s002290170024. MR: 1836111. 137

[Mat80] Hideyuki Matsumura. *Commutative algebra*. Second edition. Math. Lecture Note Ser., Vol. 56. Reading, MA: Benjamin/Cummings Publishing Co., Inc., 1980. 1970 edition available at ark:/13960/s2gv47f226m. MR: 575344. 165

[Mat89] ———. *Commutative ring theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Stud. Adv. Math., Vol. 8. Cambridge: Cambridge Univ. Press, 1989. DOI: 10.1017/CBO9781139171762. MR: 1011461. 27, 159, 168

[McQ79] Donald L. McQuillan. "On prime ideals in ring extensions." *Arch. Math. (Basel)* 33.2 (1979), pp. 121–126. DOI: 10.1007/BF01222734. MR: 557742. 52

[MS80] Masayoshi Miyanishi and Tohru Sugie. "Affine surfaces containing cylinderlike open sets." *J. Math. Kyoto Univ.* 20.1 (1980), pp. 11–42. DOI: 10.1215/kjm/1250522319. MR: 564667. 46

[Mun00] James R. Munkres. *Topology*. Second edition. Upper Saddle River, NJ: Prentice Hall, Inc., 2000. MR: 3728284. 13, 41

[Mus72] C. Musili. "Postulation formula for Schubert varieties." *J. Indian Math. Soc. (N.S.)* 36 (1972), pp. 143–171. MR: 330177. 151

[MW83] David W. Masser and Gisbert Wüstholz. "Fields of large transcendence degree generated by values of elliptic functions." *Invent. Math.* 72.3 (1983), pp. 407–464. DOI: 10.1007/BF01398396. MR: 704399. 72

[Nag56] Masayoshi Nagata. "A general theory of algebraic geometry over Dedekind domains. I. The notion of models." *Amer. J. Math.* 78.1 (1956), pp. 78–116. DOI: 10.2307/2372486. MR: 82725. 68

[Nag75] ———. *Local rings*. Corrected reprint. Huntington, NY: Robert E. Krieger Publishing Co., 1975. ark:/13960/s2r2641wnj6. MR: 460307. 27, 78, 183

[Nak51] Tadasi Nakayama. "A remark on finitely generated modules." *Nagoya Math. J.* 3 (1951), pp. 139–140. DOI: 10.1017/S0027763000012265. MR: 43770. 26

[NB14] Luis Núñez-Betancourt. "Associated primes of local cohomology of flat extensions with regular fibers and Σ-finite D-modules." *J. Algebra* 399 (2014), pp. 770–781. DOI: 10.1016/j.jalgebra.2013.10.010. MR: 3144611. 137

[Noe1921] Emmy Noether. "Idealtheorie in Ringbereichen." *Math. Ann.* 83.1-2 (1921), pp. 24–66. DOI: 10.1007/BF01464225. MR: 1511996. 1, 4, 125

[Noe26] ———. "Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p." *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1926 (1926), pp. 28–35. URL: http://eudml.org/doc/59193. ZBL: 52.0106.01. 67

[Noe27] ———. "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern." *Math. Ann.* 96.1 (1927), pp. 26–61. DOI: 10.1007/BF01209152. MR: 1512304. 26, 45

[OCa87] Liam O'Carroll. "A uniform Artin-Rees theorem and Zariski's main lemma on holomorphic functions." *Invent. Math.* 90.3 (1987), pp. 647–652. DOI: 10.1007/BF01389183. MR: 914854. 187

[OCa91] ———. "A note on Artin-Rees numbers." *Bull. London Math. Soc.* 23.3 (1991), pp. 209–212. DOI: 10.1112/blms/23.3.209. MR: 1123327. 187

[Pal04] Bruce P. Palka. "Editor's Endnotes." *Amer. Math. Monthly* 111.5 (2004), pp. 456–460. DOI: 10.1080/00029890.2004.11920101. 70

[Poo19] Bjorn Poonen. "Why all rings should have a 1." *Math. Mag.* 92.1 (2019), pp. 58–62. DOI: 10.1080/0025570X.2018.1538714. MR: 3914018. 1

[Rab30] J. L. Rabinowitsch. "Zum Hilbertschen Nullstellensatz." *Math. Ann.* 102.1 (1930), p. 520. DOI: 10.1007/BF01782361. MR: 1512592. 70

[Ree56a] David Rees. "Two classical theorems of ideal theory." *Proc. Cambridge Philos. Soc.* 52 (1956), pp. 155–157. DOI: 10.1017/s0305004100031091. MR: 74386. 183

[Ree56b] ———. "Valuations associated with ideals. II." *J. London Math. Soc.* 31 (1956), pp. 221–228. DOI: 10.1112/jlms/s1-31.2.221. MR: 78971. 183

[Rei95] Miles Reid. *Undergraduate commutative algebra*. London Math. Soc. Stud. Texts, Vol. 29. Cambridge: Cambridge Univ. Press, 1995. DOI:

10.1017/CBO9781139172721. MR: 1458066. xi, xiii, 1, 2, 4, 11, 12, 14, 15, 29, 40, 47, 65–67, 81–83, 85, 125–128, 130, 131, 133, 158, 164–168

[Ros73] Michael Rosen. "S-units and S-class group in algebraic function fields." *J. Algebra* 26 (1973), pp. 98–108. DOI: 10.1016/0021-8693(73)90036-7. MR: 327777. 163

[Ros76] _____. "Elliptic curves and Dedekind domains." *Proc. Amer. Math. Soc.* 57.2 (1976), pp. 197–201. DOI: 10.2307/2041187. MR: 417190. 163

[Rud82] Lee Rudolph. "Embeddings of the line in the plane." *J. Reine Angew. Math.* 337 (1982), pp. 113–118. DOI: 10.1515/crll.1982.337.113. MR: 676044. 3

[Rus81] Peter Russell. "On affine-ruled rational surfaces." *Math. Ann.* 255.3 (1981), pp. 287–302. DOI: 10.1007/BF01450704. MR: 615851. 46

[Sam64] Pierre Samuel. "Anneaux gradués factoriels et modules réflexifs." *Bull. Soc. Math. France* 92 (1964), pp. 237–249. NUMDAM: BSMF_1964__92__237_0. MR: 186702. 150

[Sch22] Peter Scholze. "Étale cohomology of diamonds." Jan. 27, 2022. arXiv: 1709.07343v3 [math.AG]. 43

[SH06] Irena Swanson and Craig Huneke. *Integral closure of ideals, rings, and modules*. London Math. Soc. Lecture Note Ser., Vol. 336. Cambridge: Cambridge Univ. Press, 2006. Corrected online version available at https://www.math.purdue.edu/~iswanso/book. MR: 2266432. 52

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1. Varieties in projective space*. Third edition. Translated from the 2007 third Russian edition by Miles Reid. Heidelberg: Springer, 2013. DOI: 10.1007/978-3-642-37956-7. MR: 3100243. 42

[Sha16] Rodney Y. Sharp. "David Rees, FRS 1918–2013." *Bull. Lond. Math. Soc.* 48.3 (2016), pp. 557–576. DOI: 10.1112/blms/bdw010. MR: 3509915. 183

[Shi89] Bernard Shiffman. "Degree bounds for the division problem in polynomial ideals." *Michigan Math. J.* 36.2 (1989), pp. 163–171. DOI: 10.1307/mmj/1029003939. MR: 1000520. 72

[Som99] Martín Sombra. "A sparse effective Nullstellensatz." *Adv. in Appl. Math.* 22.2 (1999), pp. 271–295. DOI: 10.1006/aama.1998.0633. MR: 1659402. 73

[Stacks] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2025. 114

[Suz74] Masakazu Suzuki. "Propriétés topologiques des polynômes de deux variables complexes, et automorphismes algébriques de l'espace $\mathbf{C}^2$." *J. Math. Soc. Japan* 26 (1974), pp. 241–257. DOI: 10.2969/jmsj/02620241. MR: 338423. 3

[Swa62] Richard G. Swan. "Vector bundles and projective modules." *Trans. Amer. Math. Soc.* 105 (1962), pp. 264–277. DOI: 10.2307/1993627. MR: 143225. 113

[Tem08] Michael Temkin. "Desingularization of quasi-excellent schemes in characteristic zero." *Adv. Math.* 219.2 (2008), pp. 488–522. DOI: 10.1016/j.aim.2008.05.006. MR: 2435647. 187

[Tho86] Mary L. Thompson. *Topics in the ideal theory of commutative Noetherian rings*. Ph.D. thesis. University of Michigan, 1986, 56 pp. URL: https://www.proquest.com/docview/303490832. MR: 2634812. 10, 72, 151

[Vak] Ravi Vakil. *The rising sea. Foundations of algebraic geometry*. To be published (2025) by Princeton Univ. Press, Princeton, NJ. Draft version of Sep. 8, 2024 available at https://math.stanford.edu/~vakil/216blog/FOAGsep0824public.pdf. 164

[Vas68] Wolmer V. Vasconcelos. "Reflexive modules over Gorenstein rings." *Proc. Amer. Math. Soc.* 19 (1968), pp. 1349–1355. DOI: 10.2307/2036210. MR: 237480. 150

[vdE00] Arno van den Essen. *Polynomial automorphisms and the Jacobian conjecture*. Progr. Math., Vol. 190. Basel: Birkhäuser Verlag, 2000. DOI: 10.1007/978-3-0348-8440-2. MR: 1790619. 4

[Web1893] Heinrich Weber. "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie." *Math. Ann.* 43.4 (1893), pp. 521–549. DOI: 10.1007/BF01446451. MR: 1510818. 1, 2

[Yon54] Nobuo Yoneda. "On the homology theory of modules." *J. Fac. Sci. Univ. Tokyo Sect. I* 7 (1954), pp. 193–227. MR: 68832. 59

[Yos57] Michio Yoshida. "Some remarks on Noetherian rings." *Canadian J. Math.* 9 (1957), pp. 35–37. DOI: 10.4153/CJM-1957-005-0. MR: 82968. 183

[Zar47] Oscar Zariski. "A new proof of Hilbert's Nullstellensatz." *Bull. Amer. Math. Soc.* 53 (1947), pp. 362–368. DOI: 10.1090/S0002-9904-1947-08801-7. MR: 20075. 68

[Zor35] Max Zorn. "A remark on method in transfinite algebra." *Bull. Amer. Math. Soc.* 41.10 (1935), pp. 667–670. DOI: 10.1090/S0002-9904-1935-06166-X. MR: 1563165. 11

[ZS75] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. I*. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition. Grad. Texts in Math., Vol. 28. New York-Heidelberg-Berlin: Springer-Verlag, 1975. 1958 edition available at ark:/13960/t7rp0zh6n. MR: 384768. 138