Commutative Algebra

Math 225 Winter 2021

Eloísa Grifo
University of California, Riverside

December 30, 2020

Warning!

Proceed with caution. These notes are under construction and are 100% guaranteed to contain typos. If you find any typos or incorrections, I will be most grateful to you for letting me know. If you are looking for a place where to learn commutative algebra, I strongly recommend the following excellent resources:

- Mel Hochster's Lecture notes
- Jack Jeffries' Lecture notes (either his UMich 614 notes or his CIMAT notes)
- Atiyah and MacDonald's *Commutative Algebra* [AM69]
- Matsumura's *Commutative Ring Theory* [Mat89], or his other less known book *Commutative Algebra* [Mat80]
- Eisenbud's *Commutative Algebra with a view towards algebraic geometry* [Eis95]

The notes you see here are adapted from Jack Jeffries' notes, and inspired by all the other resources above.

Contents

Chapter 0

Setting the stage

In this chapter we set the stage for what's to come in the rest of the class. The definitions and facts we collect here should be somewhat familiar to you already, and so we present them in rapid fire succession. You can learn more about the basic theory of (commutative) rings and R-modules in any introductory algebra book, such as [DF04].

0.1 Basic definitions: rings and ideals

Roughly speaking, Commutative Algebra is the branch of algebra that studies commutative rings and modules over such rings. For a commutative algebraist, every ring is commutative and has a $1 \neq 0$.

Definition 0.1 (Ring)**.** A **ring** is a set R equipped with two binary operations $+$ and $\cdot$ satisfying the following properties:

1) R is an abelian group under the addition operation $+$, with additive identity 0.[1] Explicitly, this means that

    - $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$,
    - $a + b = b + a$ for all $a, b \in R$,
    - there is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$, and
    - for each $a \in R$ there exists an element $-a \in R$ such that $a+(-a) = 0$.

[1] Or 0_R if we need to specify which ring we are talking about.

2) R is a commutative monoid under the multiplication operation $\cdot$, with multiplicative identity 1.[2] Explicitly, this means that

   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$,
   - $a \cdot b = b \cdot a$ for all $a, b \in R$, and
   - there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1$ for all $a \in R$.

3) multiplication is distributive with respect to addition, meaning that

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

   for all $a, b, c \in R$.

4) $1 \neq 0$.

We typically write ab for $a \cdot b$.

While in some branches of algebra rings might fail to be commutative, we will explicitly say we have a *noncommutative ring* if that is the case, and otherwise all rings are assumed to be commutative. There also branches of algebra where rings might be assumed to not necessarily have a multiplicative identity; we recommend [Poo19] for an excellent read on the topic of *Why rings should have a 1.*

Example 0.2. Here are some examples of the kinds of rings we will be talking about.

a) The integers $\mathbb{Z}$.

b) Any quotient of $\mathbb{Z}$, which we write compactly as $\mathbb{Z}/n$.

c) A polynomial ring. When we say polynomial ring, we typically mean $R = k[x_1, \ldots, x_n]$, a polynomial ring in finitely many variables over a field k.

d) A quotient of a polynomial ring by an ideal I, say $R = k[x_1, \ldots, x_n]/I$.

e) Rings of polynomials in infinitely many variables, $R = k[x_1, x_2, \ldots]$.

[2] If we need to specify the corresponding ring, we may write 1_R.

f) Power series rings $R = k[\![x_1, \ldots, x_n]\!]$. The elements are (formal) power series $\sum_{a_i \geqslant 0} c_{a_1,\ldots,a_n} x_1^{a_1} \cdots x_n^{a_n}$.

g) While any field k is a ring, we will see that fields on their own are not very exciting from the perspective of the kinds of things we will be discussing in this class.

Definition 0.3 (ring homomorphism)**.** A map $R \xrightarrow{f} S$ between rings is a **ring homomorphism** if f preserves the operations and the multiplicative identity, meaning

- $f(a+b) = f(a) + f(b)$ for all $a, b \in R$,
- $f(ab) = f(a)f(b)$ for all $a, b \in R$, and
- $f(1) = 1$.

A bijective ring homomorphism is an **isomorphism**. We should think about a ring isomorphism as a relabelling of the elements in our ring.

Definition 0.4. A subset $R \subseteq S$ of a ring S is a **subring** if R is also a ring with the structure induced by S, meaning that the each operation on R is the restrictions of the corresponding operation on S to R, and the 0 and 1 in R are the 0 and 1 in S, respectively.

Often, we care about the ideals in a ring more than we care about individual elements.

Definition 0.5 (ideal)**.** A nonempty subset I of a ring R is an **ideal** if it is closed for the addition and for multiplication by any element in R: for any $a, b \in I$ and $r \in R$, we must have $a + b \in I$ and $ra \in I$.

The **ideal generated by** $f_1, \ldots, f_n$, denoted $(f_1, \ldots, f_n)$, is the smallest ideal containing $f_1, \ldots, f_n$, or equivalently,

$$(f_1, \ldots, f_n) = \{r_1 f_1 + \cdots r_n f_n \mid r_i \in R\}.$$

Example 0.6. Every ring has always at least 2 ideals, the zero ideal $(0) = \{0\}$ and the unit ideal $(1) = R$.

We will follow the convention that when we say *ideal* we actually mean every ideal $I \neq R$.

Exercise 1. The ideals in $\mathbb{Z}$ are the sets of multiples of a fixed integer, meaning every ideal has the form (n). In particular, every ideal in $\mathbb{Z}$ can be generated by one element.

This makes $\mathbb{Z}$ the canonical example of a **principal ideal domain**.

A **domain** is a ring with no zerodivisors, meaning that $rs = 0$ implies that $r = 0$ or $s = 0$. A **principal ideal** is an ideal generated by one element. A **principal ideal domain** or **PID** is a domain where every ideal is principal.

Exercise 2. Given a field k, $R = k[x]$ is a principal ideal domain, so every ideal in R is of the form $(f) = \{fg \mid g \in R\}$.

Exercise 3. While $R = k[x, y]$ is a domain, it is **not** a PID. We will see later that every ideal in R is finitely generated, and yet we can construct ideals in R with arbitrarily many generators!

Example 0.7. While $\mathbb{Z}[x]$ is a domain, it is also **not** a PID. For example, $(2, x)$ is not a principal ideal.

In commutative algebra, prime ideals play a very special role.

Definition 0.8 (prime ideal)**.** An ideal P is prime if $ab \in P$ implies $a \in P$ or $b \in P$.

Example 0.9. The prime ideals in $\mathbb{Z}$ are those of the form (p) for p a prime integer, and (0).

Exercise 4. An ideal P in R is prime if and only if R/P is a domain.

Definition 0.10 (maximal ideal)**.** An ideal $\mathfrak{m}$ in R is **maximal** if any ideal $I \supseteq \mathfrak{m}$ must satisfy $I = \mathfrak{m}$ or $I = R$.

Exercise 5. An ideal $\mathfrak{m}$ in R is maximal if and only if $R/\mathfrak{m}$ is a field.

Exercise 6. Every maximal ideal is prime.

Exercise 7. Not every prime ideal is maximal. For example, in $\mathbb{Z}$, (0) is a prime ideal that is not maximal.

Definition 0.11. An element $f \in R$ is a unit if f is invertible, or equivalently if $(f) = R$. An element $f \in R$ is **regular**, or a **nonzerodivisor**, if $fr = 0$ implies $r = 0$.

0.2 Basic definitions: modules

Similarly to how linear algebra is the study of vector spaces over fields, commutative algebra often focuses on the structure of modules over a given commutative ring R. While in other branches of algebra modules might be left- or right-modules, all our modules are two sided, and we refer to them simply as modules.

Definition 0.12 (Module)**.** Given a ring R, an **R-module** $(M, +)$ is an abelian group equipped with an R-action that is compatible with the group structure. More precisely, there is an operation $\cdot : R \times M \longrightarrow M$ such that

- $r \cdot (a + b) = r \cdot a + r \cdot b$ for all $r \in R$ and $a, b \in M$,
- $(r + s) \cdot a = r \cdot a + s \cdot a$ for all $r, s \in R$ and $a \in M$,
- $(rs) \cdot a = r \cdot (s \cdot a)$ for all $r, s \in R$ and $a \in M$, and
- $1 \cdot a = a$ for all $a \in M$.

We typically write ra for $r \cdot a$. We denote the additive identity in M by 0, or 0_M if we need to distinguish it from 0_R.

The definitions of submodule, quotient of modules, and homomorphism of modules are very natural and easy to guess, but here they are.

Definition 0.13. If $N \subseteq M$ are R-modules with compatible structures, we say that M is a **submodule** of M.

A map $M \xrightarrow{f} N$ between R-modules is a **homomorphism of R-modules** if it is a homomorphism of abelian groups that preserves the R-action, meaning $f(ra) = rf(a)$ for all $r \in R$ and all $a \in M$. We sometimes refer to R-module homomorphisms as **R-module maps**, or **maps of R-modules**. An isomorphism of R-modules is a bijective homomorphism, which we really should think about as a relabeling of the elements in our module. If two modules M and N are isomorphic, we write $M \cong N$.

Given an R-module M and a submodule $N \subseteq M$, the **quotient** M/N is an R-module whose elements are the equivalence classes determined by the relation on M given by $a \sim b \Leftrightarrow a - b \in N$. One can check that this set naturally inherits an R-module structure from the R-module structure on M, and it comes equipped with a natural **canonical map** $M \longrightarrow M/N$ induced by sending 1 to its equivalence class.

Example 0.14. The modules over a field k are precisely all the k-vector spaces. Linear transformations are precisely all the k-module maps.

While vector spaces make for a great first example, be warned that many of the basic facts we are used to from linear algebra are often a little more subtle in commutative algebra. These differences are features, not bugs.

Example 0.15. When we think of the ring R as a module over itself, the submodules of R are precisely the ideals of R.

Exercise 8. The kernel $\ker f$ and image $\operatorname{im} f$ of an R-module homomorphism $M \xrightarrow{f} N$ are submodules of M and N, respectively.

Theorem 0.16 (First Isomorphism Theorem)**.** *Given a homomorphism of R-modules $M \xrightarrow{f} N$, $M/\ker f \cong M$.*

The first big noticeable difference between vector spaces and more general R-modules is that while every vector space has a basis, most R-modules do not.

Definition 0.17. A subset $\Gamma \subseteq M$ of an R-module M is a **generating set**, or a **set of generators**, if every element in M can be written as a finite linear combination of elements in M with coefficients in R. A **basis** for an R-module M is a generating set Γ for M such that $\sum_i a_i \gamma_i = 0$ implies $a_i = 0$ for all i. An R-module is **free** if it has a basis.

Remark 0.18. Every vector space is a free module.

Remark 0.19. Every free R-module is isomorphic to a direct sum of copies of R. Indeed, let's construct such an isomorphism for a given free R-module M. Given a basis $\Gamma = \{\gamma_i\}_{i \in I}$ for M, let

$$\begin{aligned} \textstyle\bigoplus_{i \in I} R &\xrightarrow{\pi} M \\ (r_i)_{i \in I} &\longmapsto \sum_i r_i \gamma_i \end{aligned} \quad .$$

The condition that Γ is a basis for M can be restated into the statement that π is an isomorphism of R-modules.

One of the key things that makes commutative algebra so rich and beautiful is that most modules are in fact *not* free. In general, every R-module has a generating set — for example, M itself. Given some generating set Γ for M, we can always repeat the idea above and write a **presentation** $\oplus_{i \in I} R \xrightarrow{\pi} M$ for M, but in general the resulting map π will have a nontrivial kernel. A nonzero kernel element $(r_i)_{i \in I} \in \ker \pi$ corresponds to a **relation** between the generators of M.

Remark 0.20. Given a set of generators for an R-module M, any homomorphism of R-modules $M \longrightarrow N$ is determined by the images of the generators.

We say that a module is **finitely generated** if we can find a finite generating set for M. The simplest finitely generated modules are the cyclic modules.

Example 0.21. An R-module is **cyclic** if it can be generated by one element. Equivalently, we can write M as a quotient of R by some ideal I. Indeed, given a generator m for M, the kernel of the map $R \xrightarrow{\pi} M$ induced by $1 \mapsto m$ is some ideal I. Since we assumed that m generates M, π is automatically surjective, and thus induces an isomorphism $R/I \cong M$.

Similarly, if an R-module has n generators, we can naturally think about it as a quotient of R^n by the submodule of relations among those n generators.

0.3 Why study commutative algebra?

There are many reasons why one would want to study commutative algebra. For starters, it's fun! Also, modern commutative algebra has connections with many fields of mathematics, including:

- Algebra Geometry
- Algebraic Topology
- Homological Algebra
- Category Theory
- Number Theory
- Arithmetic Geometry
- Combinatorics
- Invariant Theory
- Representation Theory
- Differential Algebra
- Lie Algebras
- Cluster Algebras

Chapter 1

Finiteness conditions

1.1 Noetherian rings and modules

The most common assumption in commutative algebra is to require that our rings be Noetherian. Noetherian rings are named after Emmy Noether, who is in many ways the mother of modern commutative algebra. Many rings that one would naturally want to study are noetherian.

Definition 1.1 (Noetherian ring)**.** A ring R is *Noetherian* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

eventually stabilizes: there is some N for which $I_n = I_{n+1}$ for all $n \geqslant N$.

This condition can be restated in various equivalent forms.

Proposition 1.2. *Let R be a ring. The following are equivalent:*

1) R is a Noetherian ring.

2) Every nonempty family of ideals has a maximal element (under $\subseteq$).

3) Every ascending chain of finitely generated ideals of R stabilizes.

4) Given any generating set S for an ideal I, the ideal I is generated by a finite subset of S.

5) Every ideal of R is finitely generated.

Proof.

(1)⇒(2): We prove the contrapositive. Suppose there is a nonempty family of ideals with no maximal element. This means that we can keep inductively choosing larger ideals from this family to obtain an infinite properly ascending chain.

(2)⇒(1): An ascending chain of ideals is a family of ideals, and the maximal ideal in the family indicates where our chain stabilizes.

(1)⇒(3): Clear.

(3)⇒(4): Let's prove the contrapositive. Suppose that there is an ideal I and a generating set S for I such that no finite subset of S generates I. So for any finite $S' \subseteq S$ we have $(S') \subsetneq (S) = I$, so there is some $s \in S \smallsetminus (S')$. Thus, $(S') \subsetneq (S' \cup \{s\})$. Inductively, we can continue this process to obtain an infinite proper chain of finitely generated ideals, contradicting (3).

(4)⇒(5): Clear.

(5)⇒(1): Given an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

let $I = \bigcup_{n \in \mathbb{N}} I_n$. In general, the union of two ideals might fail to be an ideal, but the union of a chain of ideals is an ideal (exercise). By assumption, the ideal I is finitely generated, say $I = (a_1, \ldots, a_t)$, and since each a_i is in some I_{n_i}, there is an N such that every a_i is in I_N. But then $I_N = I$, and thus $I_n = I_{n+1}$ for all $n \geqslant N$. □

Example 1.3.

1) If K is a field, the only ideals in K are (0) and $(1) = K$, so K is Noetherian.

2) $\mathbb{Z}$ is a Noetherian ring. More generally, if R is a PID, then R is Noetherian. Indeed, every ideal is finitely generated!

3) As a special case of the previous example, consider the ring of germs of complex analytic functions near 0,

$$\mathbb{C}\{z\} := \{f(z) \in \mathbb{C}[\![z]\!] \mid f \text{ is analytic on a neighborhood of } z = 0\}.$$

This ring is a PID: every ideal is of the form (z^n), since any $f \in \mathbb{C}\{z\}$ can be written as $z^n g(z)$ for some $g(z) \neq 0$, and any such $g(z)$ is a unit in $\mathbb{C}\{z\}$.

4) A ring that is *not* Noetherian is a polynomial ring in infinitely many variables over a field K: the ascending chain of ideals

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$

does *not* stabilize.

5) The ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots]$ is also *not* Noetherian . A nice ascending chain of ideals is

$$(x) \subseteq (x^{1/2}) \subseteq (x^{1/3}) \subseteq (x^{1/4}) \subseteq \cdots .$$

6) The ring of continuous real-valued functions $\mathcal{C}(\mathbb{R}, \mathbb{R})$ is *not* Noetherian: the chain of ideals

$$I_n = \{f(x) \mid f|_{[-1/n,1/n]} \equiv 0\}$$

is increasing and proper. The same construction shows that the ring of infinitely differentiable real functions $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ is not Noetherian: properness of the chain follows from, e.g., Urysohn's lemma (though it's not too hard to find functions distinguishing the ideals in the chain). Note that if we asked for analytic functions instead of infinitely-differentiable functions, every element of the chain would be the zero ideal!

Remark 1.4. If R is Noetherian, and I is an ideal of R, then R/I is Noetherian as well, since there is an order-preserving bijection

$$\{\text{ideals of } R \text{ that contain } I\} \longleftrightarrow \{\text{ideals of } R/I\}.$$

This gives us many more examples, by simply taking quotients of the examples above. We will also see huge classes of easy examples once we learn about localization.

Similarly, we can define noetherian modules.

Definition 1.5 (Noetherian module)**.** An R-module M is *Noetherian* if every ascending chain of submodules of M eventually stabilizes.

There are analogous equivalent definitions for modules as we had above for rings, so we leave the proof as an exercise.

Proposition 1.6 (Equivalence definitions for Noetherian module)**.** *Let M be an R-module. The following are equivalent:*

1) M is a Noetherian module.

2) Every nonempty family of submodules has a maximal element.

3) Every ascending chain of finitely generated submodules of M eventually stabilizes.

4) Given any generating set S for a submodule N, the submodule N is generated by a finite subset of S.

5) Every submodule of M is finitely generated.

In particular, a Noetherian module must be finitely generated.

Lemma 1.7. *Let M be a module, and M', M'', and N be submodules of M.*

1) $M' = M''$ if and only if $M' \cap N = M'' \cap N$ and $M'/(M' \cap N) = M''/(M'' \cap N)$.

2) M is Noetherian if and only if N and M/N Noetherian.

Proof.

1) $(\Rightarrow)$ is clear, so we prove $(\Leftarrow)$. Suppose that $M' \subsetneq M''$ and $M' \cap N = M'' \cap N$. Then there is some element $m \in M'' \setminus M'$. We claim that the class of m in $M''/(M'' \cap N)$ is not equal to the class of m' in $M''/(M'' \cap N)$ for any $m' \in M'$. Indeed, if it were, then $m - m' \in M'' \cap N = M' \cap N$, so that $m \in M' + M' \cap N = M'$, a contradiction.

2) A chain of submodules of N is a chain of submodules of M, and a (proper) chain of submodules of M/N lifts to a (proper) chain of submodules of M, so M Noetherian implies N and M/N are also Noetherian. Conversely, if N and M/N are Noetherian, then for any chain

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

of submodules of M, the chains

$$(M_0 \cap N) \subseteq (M_1 \cap N) \subseteq (M_2 \cap N) \subseteq \cdots$$

in N and

$$\frac{M_0}{M_0 \cap N} \subseteq \frac{M_1}{M_1 \cap N} \subseteq \frac{M_2}{M_2 \cap N} \subseteq \cdots$$

in M/N stabilize eventually. If both chains are stable past index N, then the chain in M is stable past index N by 1). $\square$

Proposition 1.8. *Let R be a Noetherian ring. Given an an R-module M, M is a Noetherian module if and only if M is finitely generated.*

Consequently, if R is Noetherian, then any submodule of a finitely generated R-module is also finitely generated.

Proof. If M is Noetherian, M is finitely generated by the equivalent definitions above, and so are all of its submodules.

Now let R be Noetherian and M be a finitely generated R-module, and let's show that M is noetherian. First, we show that the free module $R^{\oplus n} = \bigoplus_{i=1}^n Re_i$ is Noetherian for all $n \in \mathbb{N}$ by induction on n. For the base case, we note that R is a Noetherian ring iff the free cyclic module $R^{\oplus 1}$ is a Noetherian module, since ideals of R correspond to submodules of $R^{\oplus 1}$. The inductive step follows since we have an isomorphism $(\bigoplus_{i=1}^n Re_i)/Re_n \cong \bigoplus_{i=1}^{n-1} Re_i$. Now, a finitely generated module M is quotient of a finitely generated free module, so is Noetherian by the previous lemma. □

Corollary 1.9. *If a ring R is a module-finite extension of a noetherian ring A, then R is also a noetherian ring.*

Proof. By , R is a Noetherian A-module, and any ideal of R is an A-submodule of R, so an ascending chain necessarily stabilizes.

□

David Hilbert had a big influence in the early years of commutative algebra, in many different ways. Emmy Noether's early work in algebra was in part inspired by some of his own work, and he later invited Emmy Noether to join the Göttingen Math Department — many of her amazing contributions to algebra happened during her time in Göttingen. Unfortunately, some of the faculty was opposed to having a woman joining the department, and for her first two years in Góttingen Noether did not have an official position nor was she paid. Hilbert's contributions also include three of the most fundamental results in commutative algebra — Hilbert's Basis Theorem, the Hilbert Syzygy Theorem, and Hilbert's Nullstellensatz. We can now prove the first.

Theorem 1.10 (Hilbert's Basis Theorem)**.** *Let A be a Noetherian ring. Then the rings $A[x_1, \ldots, x_d]$ and $A[\![x_1, \ldots, x_d]\!]$ are Noetherian..*

Remark 1.11. We can rephrase this theorem in a way that can be understood by anyone with a basic high school algebra (as opposed to abstract algebra) knowledge:

> Any system of polynomial equations in finitely many variables can be written in terms of finitely many equations.

Proof. We give the proof for polynomial rings, and indicate the difference in the power series argument.

Using induction on d, we can reduce to the case $d = 1$. Let $I \subseteq A[x]$, and let

$$J = \{a \in A \mid \exists\, ax^n + \text{lower order terms (wrt } x) \in I\}.$$

So $J \subseteq R$ consists of all the leading coefficients of polynomials in I. We can check (exercise) that this is an ideal of A. By our hypothesis, J is finitely generated, so let $J = (a_1, \ldots, a_t)$. Pick $f_1, \ldots, f_t \in A[x]$ such that the leading coefficient of f_i is a_i, and set $i' = \gcd(f_1, \ldots, f_t)$. Let $N = \max_i \deg f_i$.

Given any $f \in I$ of degree greater than N, we can cancel off the leading term of f by subtracting a suitable multiple of some f_i, so any $f \in I$ can be written as $g + h$ with $g \in I \cap \sum_{i=0}^{N} Ax^i$ and $h \in I'$. Since $I \cap \sum_{i=0}^{N} Ax^i$ is a submodule of a finitely generated free A-module, it is also finitely generated as an A-module. Given such a generating set, we can clearly write any such f as an $A[x]$-linear combination of these generators and the f_i's.

In the power series case, take J to be the coefficients of *lowest degree* terms. $\square$

1.2 Algebras

If R is a subring of S, then S is an **algebra** over R, meaning that S is a ring with a (natural) structure of an S-module. More generally, given any ring homomorphism $\varphi : R \to S$, S is an algebra over R via φ, by setting $r \cdot s = \varphi(r)s$. We may abuse notation and write $r \in S$ for its image $\varphi(r) \in S$.

Giving a ring homomorphism $R \to S$ is the same as giving an R-algebra. In particular, a ring S can have different R-algebra structures given by different homomorphisms $R \to S$.

A set of elements $\Lambda \subseteq S$ **generates** S as an R-algebra if the following equivalent conditions hold:

- The only subring of S containing $\varphi(R)$ and Λ is S itself.
- Every element of S admits a polynomial expression in Λ with coefficients in $\varphi(R)$.

- Given a polynomial ring $R[X]$ on $|\Lambda|$ indeterminates, the homomorphism
$$\begin{aligned} R[X] &\xrightarrow{\psi} S \\ x_i &\longmapsto \lambda_i \end{aligned}$$
is surjective.

We say that $\varphi : R \to S$ is **algebra-finite**, or S is a **finitely generated** R**-algebra**, or S is of **finite type** over R, if there exists a *finite* set of elements $f_1, \dots, f_t \in S$ that generates S as an R-algebra. A better name might be *finitely generatable*, since to say that an algebra is finitely generated does not require knowing any actual finite set of generators.

From the discussion above and the first isomorphism theorem, S is a finitely generated R-algebra if and only if S is a quotient of some polynomial ring $R[x_1, \dots, x_d]$ over R in finitely many variables. If S is generated over R by $f_1, \dots, f_d$, we will use the notation $R[f_1, \dots, f_d]$ to denote S. Of course, for this notation to properly specify a ring, we need to understand how these generators behave under the operations. This is no problem if A and $\underline{f}$ are understood to be contained in some larger ring.

Remark 1.12. Any surjective φ is algebra-finite, since the target is generated by 1. Moreover, any homomorphism $\varphi : R \to S$ can be factored as the surjection $R \to R/\ker(\varphi)$ followed by the inclusion $R/\ker(\varphi) \hookrightarrow S$, so to understand algebra-finiteness it suffices to restrict our attention to injective homomorphisms.

Example 1.13. Every ring is a $\mathbb{Z}$-algebra, but generally not a finitely generated one.

Remark 1.14. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $$\begin{matrix} A \subseteq B \text{ algebra-finite} \\ \text{and} \\ B \subseteq C \text{ algebra-finite} \end{matrix} \quad \Longrightarrow \quad A \subseteq C \text{ algebra-finite}$$

- $A \subseteq C$ algebra-finite $\Longrightarrow$ $B \subseteq C$ algebra-finite.

However, $A \subseteq C$ algebra-finite $\not\Longrightarrow$ $A \subseteq B$ algebra-finite.

Example 1.15. Let k be a field and

$$B = k[x, xy, xy^2, xy^3, \cdots] \subseteq C = k[x, y],$$

where x and y are indeterminates. While B and C are both k-algebras, C is a finitely generated k-algebra, while B is not. Indeed, any finitely generated subalgebra of B is contained in $K[x, xy, \ldots, xy^m]$ for some m, since we can write the elements in any finite generating set as polynomial expressions in finitely many of the specified generators of B. However, note that every element of $k[x, xy, \ldots, xy^m]$ is a k-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated A-algebra.

Let S be an R-algebra and $\Lambda \subseteq S$. The ideal of **relations** on the elements Λ over R is the kernel of the map

$$\begin{aligned} R[X] &\xrightarrow{\psi} S \\ x_i &\longmapsto \lambda_i \end{aligned}.$$

This consists of the polynomial functions with R-coefficients that the elements of Λ satisfy. Given an R-algebra S with generators Λ and ideal relations I, we have $S \cong R[X]/I$ by the first isomorphism theorem. Thus, if we understand R and generators and relations for S over R, we can get a pretty concrete understanding of S. If a sequence of elements has no nonzero relations, we say they are *algebraically independent* over A.

There are many basic questions about algebra generators that are surprisingly difficult. Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and $f_1, \ldots, f_n \in R$. When do $f_1, \ldots, f_n$ generate R over $\mathbb{C}$? It isn't too hard to show that the Jacobian determinant

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

must be a nonzero constant. It is a big open question whether this is in fact a sufficient condition!

Finally, note that an easy corollary of the Hilbert Basis Theorem is that finitely generated algebras over noetherian rings are also noetherian.

Corollary 1.16. *If R is a Noetherian ring, then any finitely generated R-algebra is Noetherian. In particular, any finitely generated algebra over a field is Noetherian.*

Proof. By our discussion above, a finitely generated R-algebra is isomorphic to a quotient of a polynomial ring over R in finitely many variables; polynomial rings over noetherian rings are Noetherian, by Hilbert's Basis Theorem, and quotients of Noetherian rings are Noetherian. □

The converse to this statement is false: there are lots of Noetherian rings that are not finitely generated algebras over a field. For example, $\mathbb{C}\{z\}$ is not algebra-finite over $\mathbb{C}$.

1.3 Integral extensions

Given a ring homomorphism $\varphi : R \to S$, saying that S acquires an R-module structure via φ by $a \cdot r = \varphi(a)r$ is a particular case of *restriction of scalars*. By restriction of scalars, we mean that any S-module M also gains a new R-module structure given by $r \cdot m = \varphi(r)m$. [1] We may write ${}_{\varphi}M$ for this R-module if we need to emphasize which map we are talking about.

Given an R-algebra S, we can consider the *algebra* structure of S over R, or its *module* structure over R. So instead of asking about how S is generated as an *algebra* over R, we can ask how it is generated as a *module* over R. Recall that an A-module M is generated by a set of elements $\Gamma \subseteq M$ if the following equivalent conditions hold:

- The smallest submodule of M that contains Γ is M itself.
- Γ generates M as an A-module.
- Every element of M admits a linear combination expression in Γ with coefficients in A.
- Given a free R-module on $|\Gamma|$ basis elements $R^{\oplus Y}$, the homomorphism

$$\begin{aligned} R^{\oplus Y} &\xrightarrow{\theta} M \\ y_i &\longrightarrow \gamma_i \end{aligned}$$

  is surjective.

[1] This gives a functor from the category of S-modules to the category of R-modules.

We use the notation $M = \sum_{\gamma \in \Gamma} A\gamma$ to indicate that M is generated by Γ as a module. We say that $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module. This is also called simply *finite* in the literature, but we'll stick with the unambiguous "module-finite."

As with algebra-finiteness, surjective maps are always module-finite in a trivial way. Thus, it suffices to understand this notion for ring inclusions.

The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression.

Example 1.17.

a) If $K \subseteq L$ are fields, saying L is module-finite over K just means that L is a finite field extension of K.

b) The Gaussian integers $\mathbb{Z}[i]$ satisfy the well-known property (or definition, depending on your source) that any element $z \in \mathbb{Z}[i]$ admits a unique expression $z = a + bi$ with $a, b \in \mathbb{Z}$. That is, $\mathbb{Z}[i]$ is generated as a $\mathbb{Z}$-module by $\{1, i\}$; moreover, they form a free module basis!

c) If R is a ring and x an indeterminate, $R \subseteq R[x]$ is not module-finite. Indeed, $R[x]$ is a free R-module on the basis $\{1, x, x^2, x^3, \dots\}$.

d) Another map that is *not* module-finite is the inclusion $K[x] \subseteq K[x, 1/x]$. Note that any element of $K[x, 1/x]$ can be written in the form $f(x)/x^n$ for some f and n. Then, any finitely generated $K[x]$-submodule M of $K[x, 1/x]$ is of the form $M = \sum_i \frac{f_i(x)}{x^{n_i}} \cdot K[x]$; taking $N = \max\{n_i \mid i\}$, we find that $M \subseteq 1/x^N \cdot K[x] \neq K[x, 1/x]$.

Lemma 1.18. *If $R \subseteq S$ is module-finite and N is a finitely generated S-module, then N is a finitely generated R-module by restriction of scalars. In particular, the composition of two module-finite ring maps is module-finite.*

Proof. Let $S = \sum_{i=1}^r Ra_i$ and $N = \sum_{j=1}^s Sb_j$. Then, $N = \sum_{i=1}^r \sum_{j=1}^s Ra_ib_j$: given $n = \sum_{j=1}^s s_jb_j$, rewrite each $s_j = \sum_{i=1}^r r_{ij}a_i$ and substitute to get $n = \sum_{i=1}^r \sum_{j=1}^s r_{ij}a_ib_j$ as an R-linear combination of the a_ib_j. $\square$

In field theory, there is a close relationship between (vector space-)finite field extensions and algebraic equations. The situation for rings is similar.

Definition 1.19 (Integral element/extension)**.** Let $\varphi : A \to R$ be a ring homomorphism, and $r \in R$. The element r is **integral** over A if there are elements $a_0, \dots, a_{n-1} \in A$ such that

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1r + a_0 = 0;$$

i.e., r satisfies an *equation of integral dependence* over A.

We say that R is *integral over* A if every $r \in R$ is integral over A.

Again, we can restrict our focus to inclusion maps $A \subseteq R$.

Remark 1.20. An element $r \in R$ is integral over A if and only if r is integral over the subring $\varphi(A) \subseteq R$.

Evidently, integral implies algebraically dependent, and the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings.

Proposition 1.21. *Let $A \subseteq R$ be rings.*

1) *If $r \in R$ is integral over A then $A[r]$ is module-finite over A.*
2) *If $r_1, \dots, r_t \in R$ are integral over A then $A[r_1, \dots, r_t]$ is module-finite over A.*

Proof.

1) Suppose r is integral over A, and $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$. Then $A[r] = A + Ar + \cdots + Ar^{n-1}$. Indeed, given a polynomial $p(r) \in A[r]$ of degree $\geqslant n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in r.
2) Write

$$A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \dots, r_t].$$

Note that r_i is integral over A_{i-1}, via the same monic equation of r_i over A. Then, the inclusion $A \subseteq A[r_1, \dots, r_t]$ is a composition of module-finite maps, and thus it is also module-finite. $\square$

The name “ring” is roughly based on this idea: in an extension as above, the powers wrap around (like a ring).

We will need a linear algebra fact. The **classical adjoint** of an $n \times n$ matrix $B = [b_{ij}]$ is the matrix $\mathrm{adj}(B)$ with entries $\mathrm{adj}(B)_{ij} = (-1)^{i+j} \det(\widehat{B_{ji}})$, where $\widehat{B_{ji}}$ is the matrix obtained from B by deleting its jth row and ith column. You may remember this matrix from linear algebra.

Lemma 1.22 (Determinant trick)**.** *Let R be a ring, $B \in M_{n \times n}(R)$, $v \in R^{\oplus n}$, and $r \in R$.*

1) $\mathrm{adj}(B)B = \det(B)I_{n\times n}$.

2) If $Bv = rv$*, then* $\det(rI_{n\times n} - B)v = 0$.

Proof.

1) When R is a field, this is a basic linear algebra fact. We deduce the case of a general ring from the field case.

   The ring R is a $\mathbb{Z}$-algebra, so we can write R as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \to R$ be a surjection, let $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that

   $$\psi(\mathrm{adj}(A)_{ij}) = \mathrm{adj}(B)_{ij} \quad \text{and} \quad \psi((\mathrm{adj}(A)A)_{ij}) = (\mathrm{adj}(B)B)_{ij},$$

   since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish 1) in the case when $R = \mathbb{Z}[X]$. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of its fraction field. Since both sides of the equation live in R and are equal in the fraction field (by linear algebra) they are equal in R.

2) We have $(rI_{n\times n} - B)v = 0$, so

   $$\det(rI_{n\times n} - B)v = \mathrm{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0. \qquad \square$$

Theorem 1.23 (Module finite implies integral)**.** *Let* $A \subseteq R$ *be module-finite. Then* R *is integral over* A*.*

Proof. Let $r \in R$. The idea is to show that multiplication by r, realized as a linear transformation over A, satisfies the characteristic polynomial of that linear transformation.

Write $R = Ar_1 + \cdots Ar_t$. We may assume that $r_1 = 1$, perhaps by adding module generators. By assumption, we can find $a_{ij} \in A$ such that

$$rr_i = \sum_{j=1}^{t} a_{ij} r_j$$

for each i. Let $C = [a_{ij}]$, and v be the column vector $(r_1, \dots, r_t)$. We then have $rv = Cv$, so by the determinant trick, $\det(rI_{n\times n} - C)v = 0$. In particular, $\det(rI_{n\times n} - C) = 0$. Exapanding as a polynomial in r, this is a monic equation with coefficients in A. $\square$

Corollary 1.24 (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): A generating set for R as an A-module serves as a generating set as an A-algebra. The rest of this direction comes from the previous theorem.
($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.21. ☐

Corollary 1.25. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

Proof. Let $R = A[\Lambda]$, with λ integral over A for all $\lambda \in \Lambda$. Given $r \in R$, there is a finite subset $L \subseteq \Lambda$ such that $r \in A[L]$. By the theorem, $A[L]$ is module-finite over A, and $r \in A[L]$ is integral over A.

For the latter statement,

$$\{\text{integral elements}\} \subseteq A[\{\text{integral elements}\}] \subseteq \{\text{integral elements}\},$$

so equality holds throughout, and {integral elements} is a ring. ☐

Definition 1.26. If $A \subseteq R$, the **integral closure of A in R** is the set of elements of R that are integral over A.

Example 1.27.

1) Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. Then S is module-finite over R: indeed, S is generated over R as an algebra by one element, z, and z satisfies the monic equation $r^2 + x^2 + y^2 = 0$, so it is integral over R.
2) Not all integral extensions are module-finite. Let $K = \overline{K}$ be an algebraically closed field, and consider $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots] \subseteq \overline{K(x)}$. Clearly R is generated by integral elements over $K[x]$, but is not algebra-finite over $K[x]$. (Prove it!)

Remark 1.28. Let $A \subseteq B \subseteq C$ be rings. As with algebra-finiteness, it follows from the definitions that

- $\begin{array}{c} A \subseteq B \text{ module-finite} \\ \text{and} \\ B \subseteq C \text{ module-finite} \end{array} \quad \Longrightarrow \quad A \subseteq C \text{ module-finite}$

- $A \subseteq C$ module-finite $\implies$ $B \subseteq C$ module-finite.

but again, $A \subseteq C$ module-finite $\not\Longrightarrow$ $A \subseteq B$ module-finite.

Finally, we can prove a technical sounding result that puts together all our finiteness conditions in a useful way.

Theorem 1.29 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

- *A is Noetherian,*
- *C is module-finite over B, and*
- *C is algebra-finite over A.*

Then, B is algebra-finite over A.

Proof. Let $C = A[f_1, \ldots, f_r]$ and $C = \sum_{i=1}^{s} Bg_i$. Then,

$$f_i = \sum b_{ij} g_j \quad \text{and} \quad g_i g_j = \sum b_{ijk} g_k$$

for some elements $b_{ij}, b_{ijk} \in B$. Let $B_0 = A[\{b_{ij}, b_{ijk}\}] \subseteq B$. Since A is Noetherian, so is B_0.

We claim that $C = \sum_{i=1}^{s} B_0\, g_i$. Given an element $c \in C$, write c as a polynomial expression in $\underline{f}$. We have that $c \in A[\{b_{ij}\}][g_1, \ldots, g_s]$. Then, using the equations for $g_i g_j$, we can write c in the form required.

Now, since B_0 is Noetherian, C is a finitely generated B_0-module, and $B \subseteq C$, then B is a finitely generated B_0-module, too. In particular, $B_0 \subseteq B$ is algebra-finite. We conclude that $A \subseteq B$ is algebra-finite, as required. $\square$

1.4 An application to invariant rings

Historically, commutative algebra has roots in classical questions of algebraic and geometric flavors, including the following natural question:

Question 1.30. Given a (finite) set of symmetries, consider the collection of polynomial functions that are fixed by all of those symmetries. Is there a finite set of fixed polynomials such that any fixed polynomial can be expressed in terms of them?

To make this precise, let G be a group acting on a ring R, or just as well, a group of automorphisms of R. The main case we have in mind is when $R = K[x_1, \dots, x_d]$ is a polynomial ring over a field. We are interested in the set of elements that are *invariant* under the action

$$R^G := \{r \in R \mid g(r) = r \text{ for all } g \in G\}.$$

If $r, s \in R^G$, then

$$r+s = g(r)+g(s) = g(r+s) \quad \text{and} \quad rs = g(r)g(s) = g(rs) \qquad \text{for all } g \in G,$$

since each g is a homomorphism. Thus, R^G is a subring of R. Note that if $G = \langle g_1, \dots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \dots, t$.

Our question can now be rephrased as

Question 1.31. Given a finite group G acting on $RK[x_1, \dots, x_d]$, is R^G a finitely generated K-algebra?

The answer is yes.

Proposition 1.32. *Let K be a field, R be a finitely-generated K-algebra, and G a finite group of automorphisms of R that fix K. Then, $R^G \subseteq R$ is module-finite.*

Proof. Since integral implies module-finite, we will show that R is algebra-finite and integral over R^G.

First, since R is generated by a finite set as a K-algebra, and $K \subseteq R^G$, it is generated by the same finite set as an R^G-algebra as well. Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g \in G}(t - g(r)) \in R[t]$. Clearly $g(F_r(t)) = F_r(t)$, where G fixes t. Thus, $F_r(t) \in R^G[t]$. The leading term (with respect to t) is $t^{|G|}$, so $F_r(t)$ is monic. Thus, r is integral over R^G. Therefore, R is integral over R^G. □

Theorem 1.33 (Noether's finiteness theorem for invariants of finite groups)**.** *Let K be a field, R be a polynomial ring over K, and G be a finite group acting K-linearly on R. Then R^G is a finitely generated K-algebra.*

Proof. Observe that $K \subseteq R^G \subseteq R$, that K is Noetherian, $K \subseteq R$ is algebra-finite, and $R^G \subseteq R$ is module-finite. Thus, by the Artin-Tate Lemma, we are done! □

Appendix A

Macaulay2

There are several computer algebra systems dedicated to algebraic geometry and commutative algebra computations, such as Singular (more popular among algebraic geometers), CoCoA (which is more popular with european commutative algebraists, having originated in Genova, Italy), and Macaulay2. There are many computations you could run on any of these systems (and others), but we will focus on Macaulay2 since it's the most popular computer algebra system among US based commutative algebraists.

Macaulay2, as the name suggests, is a successor of a previous computer algebra system named Macaulay. Macaulay was first developed in 1983 by Dave Bayer and Mike Stillman, and while some still use it today, the system has not been updated since its final release in 2000. In 1993, Daniel Grayson and Mike Stillman released the first version of Macaulay2, and the current stable version if Macaulay2 1.16.

Macaulay2, or M2 for short, is an open-source project, with many contributors writing packages that are then released with the newest Macaulay2 version. Journals like the *Journal of Software for Algebra and Geometry* publish peer-refereed short articles that describe and explain the functionality of new packages, with the package source code being peer reviewed as well.

The National Science Foundation has funded Macaulay2 since 1992. Besides funding the project through direct grants, the NSF has also funded several Macaulay2 workshops — conferences where Macaulay2 package developers gather to work on new packages, and to share updates to the Macaulay2 core code and recent packages.

A.1 Getting started

A Macaulay2 session often starts with defining some ambient ring we will be doing computations over. Common rings such as the rationals and the integers can be defined using the commands `QQ` and `ZZ`; one can easily take quotients or build polynomial rings (in finitely many variables) over these. For example,

```
i1 : R = ZZ/101[x,y]

o1 = R

o1 : PolynomialRing
```

and

```
i1 : k = ZZ/101;

i2 : R = k[x,y];
```

both store the ring $\mathbb{Z}/101$ as R, with the small difference that in the second example Macaulay2 has named the coefficient field k. One quirk that might make a difference later is that if we use the first option and later set k to be the field $\mathbb{Z}/101$, our ring R is *not* a polynomial ring over k. Also, in the second example we ended each line with a `;`, which tells Macaulay2 to run the command but not display the result of the computation — which is in this case was simply an assignment, so the result is not relevant. Lines indicated with as in, where n is some integer, are input lines, whereas lines with an on indicate output lines.

We can now do all sorts of computations over our ring R. We can define ideals in R, and use them to either define a quotient ring S of R or an R-module M, as follows:

```
i3 : I = ideal(x^2,y^2,x*y)

               2   2
o3 = ideal (x , y , x*y)

o3 : Ideal of R
```

```
i4 : M = R^1/I

o4 = cokernel | x2 y2 xy |

                               1
o4 : R-module, quotient of R

i5 : S = R/I

o5 = S

o5 : QuotientRing
```

It's important to note that while R is a ring, R^1 is the R-module R — this is a very important difference for Macaulay2, since these two objects have different types. So S defined above is a ring, while M is a module. Notice that Macaulay2 stored the module M as the cokernel of the

$$R^3 \xrightarrow{\begin{bmatrix} x^2 & y^2 & xy \end{bmatrix}} R \, .$$

Note also that there is an alternative syntax to write our ideal I from above, as follows:

```
i15 : I = ideal"x2,xy,y2"

               2         2
o15 = ideal (x , x*y, y )

o15 : Ideal of R
```

An ideal, unfortunately, is not a module in Macaulay2. If you want to run any computations involving I that will require seeing it as a module, you can run

```
i18 : N = module I

o18 = image | x2 xy y2 |
                               1
o18 : R-module, submodule of R
```

and our newly defined N is indeed I, but viewed as an R-module.

When you make a new definition in Macaulay2, you might want to pay attention to what ring your new object is defined over. For example, now that we defined this ring S, Macaulay2 has automatically taken S to be our current ambient ring, and any calculation or definition we run next will be considered over S and not R. If you want to return to the original ring R, you must first run the command `use S`.

Many Macaulay2 commands are easy to guess, and named exactly what you would expect them to be named. If you are not sure how to use a certain command, you can run `viewHelp` followed by the command you want to ask about; this will open an html file with the documentation for the method you asked about. Often, googling "Macaulay2" followed by descriptive words will easily land you on the documentation for whatever you are trying to do.

If you want to work over a finitely generated algebra over one of the basic rings you can define in Macaulay2, and your ring is not a quotient of a polynomial ring, you want to rewrite this algebra as a quotient of a polynomial ring. For example, suppose you want to work over the 2nd Veronese in 2 variables over our field k from before, meaning the algebra $k[x^2, xy, y^2]$. We need 3 algebra generators, which we will call a, b, c, corresponding to x^2, xy, and y^2:

```
i11 : U = k[a,b,c]

o11 = U

o11 : PolynomialRing

i12 : f = map(R,U,{x^2,x*y,y^2})
                  2        2
o12 = map(R,U,{x , x*y, y })

o12 : RingMap R <--- U

i13 : J = ker f

               2
o13 = ideal(b  - a*c)
```

```
o13 : Ideal of U

i14 : T = U/J

o14 = T

o14 : QuotientRing
```

Our ring T at the end is isomorphic to the 2nd Veronese of R, which is the ring we wanted.

Index

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, 3rd ed edition, 2004.

[Eis95] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Poo19] Bjorn Poonen. Why all rings should have a 1. *Mathematics Magazine*, 92(1):58–62, 2019.