Commutative Algebra 1

Math 905 Fall 2022

Eloísa Grifo
University of Nebraska-Lincoln

September 21, 2022

Warning!

Proceed with caution. These notes are under construction and are 100% guaranteed to contain typos. If you find any typos or errors, 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]

Acknowledgements

These notes are heavily based on Jack Jeffries and Alexandra Seceleanu's notes, and I thank them for sharing their notes with me. Thank you also to all the students in my commutative algebra class at UCR in Winter 2021 for their comments and questions that lead to multiple improvements, especially Brandon Massaro, Rahul Rajkumar, Adam Richardson, Khoa Ta, Ryan Watson, and Noble Williamson, who found typos and errors. Thank you also to Julie Geraci and Jordan Barrett, both for finding typos and for their many excellent questions that lead to improvements.

Contents

Chapter 0

Setting the stage

Here are some elementary definitions and facts we will assume you have already seen before. For more details, see any introductory algebra book, such as [DF04].

0.1 Basic definitions: rings and ideals

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, or 0_R if we need to specify which ring we are talking about. 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 $a + (-a) = 0$.
2) R is a commutative monoid under the multiplication operation $\cdot$, with multiplicative identity 1_R or simply 1. 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 $a \in R$.

   We typically write ab for $a \cdot b$.
3) multiplication is distributive with respect to addition, meaning that for all $a, b, c \in R$ we have
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$
4) $1 \neq 0$.

In this class, **all rings are commutative**. In other branches of algebra rings might fail to be commutative, but we will explicitly say *noncommutative ring* if that is the case. There also branches of algebra where rings are allowed to not 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 $\mathbb{Z}$, or any quotient of $\mathbb{Z}$, which we write compactly as $\mathbb{Z}/n$.

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

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

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

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

f) 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)**.** Given rings R and S, a function $R \xrightarrow{f} S$ 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,

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

Example 0.6. Every ring has always at least two 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 an 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**.

Definition 0.7. 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 $(f) = \{fg \,|\, g \in R\}$.

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 0.8. The ring $\mathbb{Z}[x]$ is a domain but **not** a PID. For example, $(2, x)$ is not principal.

Theorem 0.9 (CRT)**.** *Let R be a ring and $I_1, \ldots, I_n$ be pairwise coprime ideals in R, meaning $I_i + I_j = R$ for all $i \neq j$. Then $I := I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$, and there is an isomorphism of rings*

$$\begin{aligned} R/I &\xrightarrow{\cong} R/I_1 \times \cdots \times R/I_n \ . \\ r + I &\longmapsto (r + I_1, \ldots, r + I_n) \end{aligned}$$

0.2 Basic definitions: modules

Just like linear algebra is the study of vector spaces over fields, commutative algebra often focuses on the structure of modules over commutative rings. While in other branches of algebra modules might be left- or right-modules, our modules are usually two sided, and we refer to them simply as modules.

Definition 0.10 (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 $r \cdot a$, and 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 0.11. If $N \subseteq M$ are R-modules with compatible structures, we say that N 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 module** M/N is an R-module whose elements are the equivalence classes under 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 0.12. The modules over a field k are precisely all the k-vector spaces. Linear transformations are precisely all the k-module maps.

Example 0.13. The $\mathbb{Z}$-modules are precisely all the abelian groups.

Example 0.14. When we think of the ring R as a module over itself, the submodules of R are precisely the ideals of R.

Exercise 4. 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 0.15 (First Isomorphism Theorem)**.** *If $M \xrightarrow{f} N$ is a homomorphism of R-modules, then $M/\ker f \cong \operatorname{im} f$.*

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

We start our study of commutative algebra by discussing modules and algebras, the most important structures over a given ring. We will discuss module-finite versus algebra-finite ring extensions, the relationship between the two concepts, and how they relate to integral extensions. We will then be ready to discuss noetherian rings; most of the rings we will be interested in are noetherian, as it often happens in commutative algebra.

1.1 Modules

In many ways, commutative algebra is the study of finitely generated modules. While vector spaces make for a great first example of modules, 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. The first big noticeable difference between vector spaces and general modules is that while every vector space has a basis, most modules do not.

Definition 1.1. Let M be an R-module and $\Gamma \subseteq M$. The **submodule** of M **generated by** Γ, denoted $\sum_{m\in\Gamma} Rm$, is the smallest (with respect to containment) submodule of M containing Γ. We say Γ **generates** M, or is a **set of generators** for M, if $\sum_{m\in\Gamma} Rm = M$, meaning that every element in M can be written as a finite linear combination of elements in Γ. 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.

Example 1.2. Every vector space over a field k is a free k-module.

Remark 1.3. Every free R-module is isomorphic to a direct sum of copies of R. To construct such an isomorphism for the free R-module M, take a basis $\Gamma = \{\gamma_i\}_{i\in I}$ for M and let

$$\begin{aligned} \oplus_{i\in I} R &\xrightarrow{\pi} M \\ (r_i)_{i\in I} &\longrightarrow \sum_i r_i\gamma_i. \end{aligned}$$

The condition that Γ is a basis for M is equivalent to π being 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 write a **presentation**

$$\begin{aligned} \oplus_{i\in I} R &\xrightarrow{\pi} M \\ (r_i)_{i\in I} &\longrightarrow \sum_i r_i\gamma_i. \end{aligned}$$

for M, but in general 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 1.4. A homomorphism of R-modules $M \longrightarrow N$ is completely determined by the images of the elements on any given set of generators for M.

Lemma 1.5. *The following are equivalent:*

1) Γ *generates* M *as an* R*-module.*

2) Every element of M *can be written as a finite linear combination of the elements of* Γ *with coefficients in* R*.*

3) The homomorphism $\theta\colon R^{\oplus Y} \to M$*, where* $R^{\oplus Y}$ *is a free* R*-module with basis* Y *in bijection with* Γ *via* $\theta(y_i) = \gamma_i$*, is surjective.*

Remark 1.6. The equivalence between 1) and 2) in Lemma 1.5 says that the submodule generated by Γ is exactly the set of all finite linear combinations of elements in Γ with coefficients in R, which explains the notation $\sum_{m\in\Gamma} Rm$.

Definition 1.7. We say that a module M is **finitely generated** if we can find a finite generating set for M.

A better name might be *finitely generatable*, since we do not need to know an actual finite set of generators to say that a module is finitely generated. The simplest finitely generated modules are the cyclic modules.

Example 1.8. 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 $R/I \cong M$.

Remark 1.9. More generally, 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. More precisely, if M is generated by $m_1, \ldots, m_n \in M$, then the homomorphism of R-modules

$$\begin{aligned} R^n &\xrightarrow{\pi} M \\ (r_1, \ldots, r_n) &\longrightarrow r_1m_1 + \cdots + r_nm_n \end{aligned}$$

that sends each of the canonical generators e_i of R^n to m_i is surjective; more precisely, this is a presentation for M. By the First Isomorphism Theorem, $M \cong R^n/\ker\pi$.

Macaulay2. Defining free modules in Macaulay2 is easy:

```
i1 : R = QQ[x,y,z];

i2 : M = R^3
      3
o2 = R

o2 : R-module, free
```

Note that from now on and until we reset Macaulay2, whenever you write `R` it will be read as a ring, not a module; if instead you want to refer to the module R, you can write it as `R^1`. Alternatively, you can also use the command `module` and write `module R`. If you do calculations that require a module and not a ring, it is important to be careful about whether you write `R` or `R^1`; this is an easy way to get an error message.

If we want to define a module that happens to be an ideal, but we want to think about it as a module, we can simply use the command `module` to turn the ideal into a module:

```
i3 : I = ideal"xy,yz"

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

o3 : Ideal of R

i4 : N = module I

o4 = image | xy yz |
                              1
o4 : R-module, submodule of R
```

If we forget that this is actually an ideal, and simply think about as a submodule of the module R, we can also view this module as the image of a map, as we described in Remark 1.9: if a submodule of R^m has n generators, we can view it as the the image of the map $R^n \to R^m$ that sends each of the canonical generators of R^n to the generators we chose for our module. In our example, our module is the image of the following map from R^2 to R:

```
i5 : phi = map(R^1,R^2,{{x*y,y*z}})

o5 = | xy yz |
             1       2
o5 : Matrix R  <--- R

i6 : L = image phi

o6 = image | xy yz |
                              1
o6 : R-module, submodule of R
```

Note that above, when we first defined the module N, Macaulay2 immediately stored that information in this exact way, as the image of the same map we just defined. This is useful to keep in mind when you see the results for a computation: if a module is given to us as the image of a matrix, then we are being told that our module is a submodule of some free module. If the matrix has n rows, then that means our module is a submodule of R^n. Each column corresponds to a generator of our module (as a submodule of R^n).

Of course that the modules M, N, and L we have defined are all the same module: the ideal (xy, yz). It is our job to know that; depending on how you ask the question, Macaulay2 might not be able to identify this. Finally, we can also describe this module by saying that it has two generators, say f and g, and there is a unique relation between them:

$$-zf + yg = 0.$$

This means that our module is the quotient of R^2 by the submodule generated by the relation $(-z, y)$. We can write this as the quotient of R^2 by the image of a map landing in R^2, meaning it is the cokernel of a map.

```
i7 : psi = map(R^2,R^1,{{-z},{y}})

o7 = | -z |
     | y  |
             2       1
o7 : Matrix R  <--- R

i8 : K = coker psi

o8 = cokernel | -z |
              | y  |
                            2
o8 : R-module, quotient of R
```

When a module is given to us in this format, as the cokernel of some matrix, we are essentially being given a presentation: the number of rows is the number of generators, while each column corresponds to a relation among those generators. If one the vector $(r_1, \ldots, r_n)$ appears in a column of the matrix, that means that the generators $m_1, \ldots, m_n$ satisfy the relation

$$r_1 m_1 + \cdots + r_n m_n = 0.$$

Keep in mind that when you do a calculation and the result is a module given to you in this format, Macaulay2 will not necessarily respond with a *minimal* presentation: one of the generators given might actually be a linear combination of the remaining ones, so there might be more generators than necessary, and there might be superfluous relations which follow as linear combinations of the others. You might be able to get rid of some superfluous generators and relations using the command `prune`. We will discuss this in more detail when we talk about local rings.

1.2 Algebras

Definition 1.10 (Algebra)**.** Given a ring R, an R-**algebra** is a ring S equipped with a ring homomorphism $\phi : R \to S$. This defines an R-module structure on S given by **restriction of scalars**: for each $r \in R$ and $s \in S$, $rs := \phi(r)s$. This R-module structure on S is compatible with the internal multiplication of S i.e.,

$$r(st) = (rs)t = s(rt) \text{ for all } r \in R, s, t \in S.$$

We will call ϕ the **structure homomorphism** of the R-algebra S.

Example 1.11.

1) If A is a ring and $x_1, \ldots, x_n$ are indeterminates, the inclusion map $A \hookrightarrow A[x_1, \ldots, x_n]$ makes the polynomial ring into an A-algebra.

2) More generally, any inclusion map $R \subseteq S$ gives S an R-algebra structure. In this case the R-module multiplication coincides with the internal (ring) multiplication on S.

3) Any ring comes with a unique structure as a $\mathbb{Z}$-algebra, since there is a unique ring homomorphism $\mathbb{Z} \to R$: the one given by $n \mapsto n \cdot 1_R$.

Definition 1.12 (algebra generation)**.** Let S be an R-algebra with structure homomorphism φ and let $\Lambda \subseteq S$ be a set. The R-**algebra generated by** a subset Λ of S, denoted $R[\Lambda]$, is the smallest (with respect to containment) subring of S containing Λ and $\varphi(R)$. A set of elements $\Lambda \subseteq S$ **generates** S as an R-algebra if $S = R[\Lambda]$.

Note that there are two different meanings for the notation $R[S]$ for a ring R and set S: one calls for a polynomial ring, and the other calls for a subring of something. If S is a subset of elements of some other larger ring which is clear from context, then we are talking about the algebra generated by S; in contrast, if S is just a set of indeterminates, then we are talking about a polynomial ring in those variables.

This can be unpackaged more concretely in a number of equivalent ways:

Lemma 1.13. *The following are equivalent:*

1) Λ *generates* S *as an* R*-algebra.*

2) Every element in S *admits a polynomial expression in* Λ *with coefficients in* $\phi(R)$*, i.e.*

$$S = \left\{ \sum_{\text{finite}} \phi(r_{i_1,\ldots,i_n}) \lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid r_l \in R, \lambda_j \in \Lambda, i_j \geqslant 0 \right\}.$$

3) If $R[X]$ *is a polynomial ring on a set of indeterminates* X *in bijection with* Λ*, then the* R*-algebra homomorphism*

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

is surjective.

Proof. Let $S = \left\{\sum_{\text{finite}} \phi(a)\lambda_1^{i_1}\cdots\lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N}\right\}$. For the equivalence between 2) and 3), we note that S is the image of π. In particular, S is a subring of R. It then follows from the definition that 1) implies 2). Conversely, any subring of R containing $\phi(A)$ and Λ certainly must contain S, so 2) implies 1). □

Let S be an R-algebra generated by Λ, let π be the surjective map in part 3) of Lemma 1.13, and let $I := \ker\pi$. By the First Isomorphism Theorem, we have a ring isomorphism $S \cong R[X]/I$. The elements of I are the **relations** among the generators in Λ. If we understand the ring R and generators and relations for S over R, we can get a pretty concrete understanding of S.

Note that the homomorphism π need not be injective. If the homomorphism π is injective (and thus an isomorphism) we say that S is a **free algebra**; a free algebra on R is isomorphic to a polynomial ring on R. The ideal $I = \ker(\pi)$ measures how far R is from being a free R-algebra and is called the set of **relations** on Λ.

Example 1.14. You may have seen this used in $\mathbb{Z}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ to describe the ring

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

The $\mathbb{Z}$-algebra generated by $\sqrt{d}$ in the most natural place, the algebraic closure of $\mathbb{Q}$, is exactly the set above. The point is that for any power $(\sqrt{d})^n$, we can always write $n = 2q+r$ with $r \in \{0, 1\}$, so $(\sqrt{d})^n = d^q(\sqrt{d})^r$ is in the algebra generated by $\mathbb{Z}$ and $\sqrt{d}$.

We can also write the one-generated $\mathbb{Z}$-algebra $\mathbb{Z}[\sqrt{d}]$ as a quotient of a polynomial ring in one variable: if d is not a perfect square, the map π in part 3) of Lemma 1.13 is

$$\begin{aligned} \mathbb{Z}[x] &\xrightarrow{\pi} \mathbb{Z}[\sqrt{d}] \\ x &\longmapsto \sqrt{d} \end{aligned}$$

and its kernel is generated by $x^2 - d$, so $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[x]/(x^2 - d)$.

Similarly, the ring $\mathbb{Z}[\sqrt[3]{d}]$ can be written as

$$\mathbb{Z}[\sqrt[3]{d}] = \{a + b\sqrt[3]{d} + c\sqrt[3]{d^2} \mid a, b, c \in \mathbb{Z}\},$$

which is a quotient of $\mathbb{Z}[x, y]$, and the map π in part 3) of Lemma 1.13 is

$$\begin{aligned} \mathbb{Z}[x] &\xrightarrow{\pi} \mathbb{Z}[\sqrt[3]{d}] \\ x &\longmapsto \sqrt[3]{d} \\ y &\longmapsto \sqrt[3]{d^2}. \end{aligned}$$

Macaulay2. Unfortunately, Macaulay2 does not understand subalgebras directly, only quotient rings. But as we have discussed, any R-algebra can be thought of as a quotient of a polynomial ring over R. For example, the Veronese algebra $V = \mathbb{Q}[x^2, xy, xz, y^2, yz, z^2]$ is a quotient of a polynomial ring over $\mathbb{Q}$ in 6 variables, since it has 6 algebra generators. More precisely, V is the image of the map

$$\begin{aligned} \mathbb{Q}[w_1, \ldots, w_6] &\xrightarrow{\pi} R \\ (w_1, \ldots, w_6) &\longmapsto (x^2, xy, xz, y^2, yz, z^2) \end{aligned}$$

so by the First Isomorphism Theorem, $V \cong \mathbb{Q}[w_1, \ldots, w_6]/\ker\pi$.

```
i4 : use R;

i5 : aux = QQ[w_1 .. w_6]

o5 = aux

o5 : PolynomialRing

i6 : p = map(R,aux,{x^2,x*y,x*z,y^2,y*z,z^2})
                    2             2        2
o6 = map (R, aux, {x , x*y, x*z, y , y*z, z })

o6 : RingMap R <--- aux

i7 : V = aux/ker p

o7 = V

o7 : QuotientRing
```

To do calculations with V, note that w_1 is actually x^2, w_2 is xy, and so on.

Definition 1.15. 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 $f_1, \ldots, f_t \in S$ that generates S as an R-algebra.

A better name might be *finitely generatable*, since we do not need to know an actual finite set of generators to say that an algebra is finitely generated. From the discussion above, we conclude that S is a finitely generated R-algebra if and only if S is a quotient of some polynomial ring $R[x_1, \ldots, x_d]$ over R in finitely many variables. If S is generated over R by $f_1, \ldots, f_d$, we will use the notation $R[f_1, \ldots, f_d]$ 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 R and $\underline{f}$ are understood to be contained in some larger ring.

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 is not 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!

1.3 Algebra-finite versus module-finite

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. We say S is **module-finite** over R if it is finitely generated as an R-module, and **algebra-finite** over R if it is finitely generated as an R-algebra. The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression.

Lemma 1.16.

- *If M is a finitely generated R-module, then any generating set for M as an R-module contains a finite subset that generates M.*
- *If the ring S is algebra-finite over R, then any generating set for S as an R-algebra contains a finite subset that also generates S as an R-algebra.*

Proof. Let Γ be a generating set for M as an R-module. If M is a finitely generated R-module, then we can find elements $f_1 \dots, f_r$ that generate M as an R-module. Since Γ generates M, for each i we can find finitely many elements $\gamma_{i,1}, \dots, \gamma_{i,n_i} \in \Gamma$ and R-coefficients $r_{i,1}, \dots, r_{i,n_i}$ such

$$f_i = r_{i,1}\gamma_{i,1} + \cdots + r_{i,n_i}\gamma_{i,n_i}.$$

The submodule N of M generated by all the $\gamma_{i,j}$ contains the elements $f_1, \dots, f_n$, but since $M = Rf_1 + \cdots + f_n$, we conclude that M is generated by those finitely many $\gamma_{i,j}$, and thus by a finite subset of Γ.

The other proof is essentially the same, with the appropriate replacements: whenever we talk about a set that generates M as an R-module, we should instead consider a set that generates S as an R-algebra, and instead of taking linear combinations of elements we should consider polynomials in those elements with R-coefficients. □

Remark 1.17. If S is an R-algebra,

- $R \subseteq S$ is algebra-finite if $S = R[f_1, \dots, f_n]$ for some $f_1, \dots, f_n \in S$.
- $R \subseteq S$ is module-finite if $S = Rf_1 + \cdots + Rf_n$ for some $f_1, \dots, f_n \in S$.

Algebra generating sets can be very different from module generating sets.

Example 1.18. Given $n \geqslant 2$, the $\mathbb{Q}$-algebra $S = \mathbb{Q}[x]/(x^n)$ is generated as an algebra by the element x. Note, however, that this is not a free $\mathbb{Q}$-algebra: x satisfies the algebra relation $x^n = 0$. When we think about it as a $\mathbb{Q}$-module, x does not generate S, since we are no longer allowed to take products of x by itself. The set $\{1, x, \dots x^n\}$ is a generating set for S as a module; this is of course the same as asking for a basis for the $\mathbb{Q}$-vector space S.

Lemma 1.19. *If S is a module-finite R-algebra, then it is also algebra-finite.*

Proof. Let $S = Rf_1 + \cdots + Rf_n$, meaning that $f_1, \dots, f_n$ is a set of module generators for S over R. Note that every R-linear combination of $f_1, \dots, f_n$ is also an element of $R[f_1, \dots, f_n]$, and thus S is a subalgebra of $R[f_1, \dots, f_n]$. On the other hand, since $f_1, \dots, f_n \in S$ and S is an R-algebra, every polynomial in $f_1, \dots, f_n$ with coefficients in R is also in S, and thus $S = R[f_1, \dots, f_n]$, so that S is algebra-finite over R. □

The converse, however, is false: it is *harder* to be module-finite than algebra-finite.

Example 1.20.

a) 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, $\{1, i\}$ is a free module basis! As a $\mathbb{Z}$-algebra, $\mathbb{Z}[i]$ is generated by i, but it is not a free $\mathbb{Z}$-algebra, since $i^2 - 1 = 0$.

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

c) Another map that is *not* module-finite is the inclusion $R := k[x] \subseteq k[x, \frac{1}{x}] =: S$. First, note that any element of $k[x, \frac{1}{x}]$ can be written in the form $\frac{f(x)}{x^n}$ for some $f \in k[x]$ and some $n \geqslant 0$. Now any finitely generated R-submodule of S is of the form

$$M = \sum_i R \cdot \frac{f_i(x)}{x^{n_i}} = \sum_i k[x] \cdot \frac{f_i(x)}{x^{n_i}}.$$

If $n := \max\{n_i\}_i$, then $M \subseteq \frac{1}{x^n} k[x] \neq k[x, \frac{1}{x}] = S$.

d) Even innocent looking examples can be quite complicated. For example, we claim that the extension $\mathbb{Z} \subseteq \mathbb{Q}$ is neither module-finite nor algebra-finite. To see that, we first claim that the set

$$P = \left\{ \frac{1}{p} \mid p \text{ prime integer} \right\}$$

generates $\mathbb{Q}$ as a $\mathbb{Z}$-algebra. The key point here is the Fundamental Theorem of Arithmetic: since any positive integer n can be written as a product $n = p_1^{a_1} \cdots p_s^{a_s}$ where the p_i are all prime and the $a_i \geqslant 0$ are nonnegative integers, we see that the rational number $\frac{m}{n} \neq 0$ can be written as

$$\frac{m}{n} = m \left(\frac{1}{p_1}\right)^{a_1} \cdots \left(\frac{1}{p_s}\right)^{a_s} \in \mathbb{Z}\left[\frac{1}{p_1}, \dots, \frac{1}{p_s}\right] \subseteq \mathbb{Z}[P].$$

On the other hand, note that any finite subset of P is contained in

$$\left\{ \frac{1}{p} \mid p \leqslant q \text{ prime integer} \right\}$$

for some fixed prime q, and that

$$\mathbb{Z}\left[\frac{1}{p} \mid p \leqslant q \text{ is prime}\right]$$

contains only rational numbers whose denominator is a product of primes smaller than q. But there are infinitely many primes, and thus this cannot be all of $\mathbb{Q}$. By Lemma 1.16, we can conclude that $\mathbb{Q}$ is not a algebra-finite over $\mathbb{Z}$. But then $\mathbb{Q}$ cannot be module-finite over $\mathbb{Z}$, by Lemma 1.19.

Lemma 1.21. *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 $S = Ra_1 + \cdots + Ra_r$ and $N = Sb_1 + \cdots + Sb_s$. Then we claim that

$$N = \sum_{i=1}^{r} \sum_{j=1}^{s} Ra_i b_j.$$

Indeed, given $n = \sum_{j=1}^{s} s_j b_j$, rewrite each $s_j = \sum_{i=1}^{r} r_{ij} a_i$ and substitute to get

$$n = \sum_{i=1}^{r} \sum_{j=1}^{s} r_{ij} a_i b_j$$

as an R-linear combination of the $a_i b_j$. □

Remark 1.22. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $\left.\begin{array}{c} A \subseteq B \text{ algebra-finite} \\ \text{and} \\ B \subseteq C \text{ algebra-finite} \end{array}\right\} \implies A \subseteq C \text{ algebra-finite}$
- $A \subseteq C$ algebra-finite $\implies B \subseteq C$ algebra-finite.

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

Example 1.23. 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. To see this, first note by Lemma 1.16 it is sufficient to show that no finite subset of $\{xy^n \mid n \geqslant 1\}$ generates B over k. Since any such subset is contained in $\{xy^n \mid 1 \leqslant n \leqslant m\}$ for some fixed mm it is sufficient to show that B is not $k[x, xy, \ldots, xy^m]$ for any m. Now note that every element of $k[x, xy, \ldots, xy^m]$ is a k-linear combination of monomials $x^i y^j$ with $j \leqslant mi$, so this ring does not contain xy^{m+1}. Therefore, B is not a finitely generated A-algebra.

Remark 1.24. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $\left.\begin{array}{c} A \subseteq B \text{ module-finite} \\ \text{and} \\ B \subseteq C \text{ module-finite} \end{array}\right\} \implies A \subseteq C \text{ module-finite}$
- $A \subseteq C$ module-finite $\implies B \subseteq C$ module-finite.

However, we will see that $A \subseteq C$ module-finite $\not\implies A \subseteq B$ module-finite. This construction is a bit more involved, so we will leave it for the problem sets.

Remark 1.25. Any surjective ring homomorphism $\varphi : R \to S$ is both algebra-finite and module-finite, since S must then be generated over R by 1. Moreover, we can always factor φ as the surjection $R \twoheadrightarrow R/\ker(\varphi)$ followed by the inclusion $R/\ker(\varphi) \hookrightarrow S$, so to understand algebra-finiteness or module-finiteness it suffices to restrict our attention to injective homomorphisms.

1.4 Integral extensions

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

Definition 1.26 (Integral element/extension)**.** Let R be an A-algebra. The element $r \in R$ is **integral** over A if there are elements $a_0, \ldots, a_{n-1} \in A$ such that

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0,$$

we say that 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.

Integral automatically implies algebraic, but the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings. This is very different to what happens over fields, where algebraic and integral are equivalent conditions.

Example 1.27. Let's see some examples of elements that are integral over $\mathbb{Z}$, and others that are not. First, consider the $\mathbb{Z}$-algebra $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mod a, b \in \mathbb{Z}\}$. The element $\sqrt{2}$ is integral over $\mathbb{Z}$, since it satisfies the equation of integral dependence $x^2 - 2 = 0$.

On the other hand, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$: if $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ are such that

$$\left(\frac{1}{2}\right)^n + a_{n-1}\left(\frac{1}{2}\right)^{n-1} + \cdots + a_0 = 0,$$

then multiplying by 2^n gives

$$1 + 2a_{n-1} + \cdots + 2^n a_0 = 0,$$

which is impossible for parity reasons (the left hand-side is odd!). Notice, in contrast, that $\frac{1}{2}$ is algebraic over $\mathbb{Z}$, since it satisfies $2x - 1 = 0$.

Definition 1.28. Consider an an inclusion of rings $A \subseteq R$. The **integral closure** of A in R is the set of elements in R that are integral over A. We say A is **integrally closed** in R if A is its own integral closure in R. The integral closure of a domain R in its field of fractions is usually denoted by $\overline{R}$. A **normal domain** is a domain R that is integrally closed in its field of fractions, meaning $R = \overline{R}$.

Example 1.29. The ring of integers $\mathbb{Z}$ is a normal domain, meaning its integral closure in its fraction field $\mathbb{Q}$ is $\mathbb{Z}$ itself. The key idea to show this is similar to the argument we used in Example 1.27 to show that $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

In fact, this is a special case of the fact that every UFD is normal.

Exercise 5. Show that every unique factorization domain is normal.

Remark 1.30. We cannot talk about the integral closure of a ring R without specifying in what extension; the integral closures of R in different extension can be very different. In Example 1.27, we saw that the integral closure of $\mathbb{Z}$ in $\mathbb{Z}[\sqrt{2}]$ contains at least $\mathbb{Z}$ and $\sqrt{2}$, while Example 1.29 says that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

When R is a domain, if we ever refer to *the* integral closure of R, it is understood that we mean the integral closure of R in its field of fractions, $\overline{R}$.

When we study integral extensions, we can can restrict our focus to inclusion maps $A \subseteq R$, just like we did with module-finite and algebra-finite extensions.

Remark 1.31. An element $r \in R$ is integral over A if and only if r is integral over the subring $\varphi(A) \subseteq R$, so we might as well assume that φ is injective.

Proposition 1.32. *Consider a ring extension $A \subseteq R$.*

1) If $r \in R$ is integral over A, then $A[r]$ is module-finite over A.

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

Proof.

1) Let r be integral over A, with $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$ for some $a_i \in A$. We claim that $A[r] = A + Ar + \cdots + Ar^{n-1}$. Since $A[r]$ is generated by all the powers r^m of r as an A-module, to show that any polynomial $p(r) \in A[r]$ is in $A + Ar + \cdots + Ar^{n-1}$ it is enough to show that $r^m \in A + Ar + \cdots + Ar^{n-1}$ for all m. Using induction on m, the base cases $1, r, \ldots, r^{n-1} \in A + Ar + \cdots + Ar^{n-1}$ are obvious. For the induction step, we need to show that $r^m \in A + Ar + \cdots + Ar^{n-1}$ for all $m \geqslant n-1$; we can do this by induction because we can use the equation above to rewrite r^m as

$$\begin{aligned} r^m &= -r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0) \\ &= -a_{n-1}r^{m-1} - \cdots a_1 r^{m-n+1} - a_0 r^{m-n}, \end{aligned}$$

which is a linear combination of powers of r of degree up to $m-1$.

2) Write

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

Since r_i is integral over A, it is also integral over A_{i-1}, via the same monic equation that r_i satisfies over A. By part 1), we conclude that the each extension $A_{i-1} \subseteq A_i$ is module-finite. Thus the inclusion $A \subseteq A[r_1, \ldots, r_t]$ is a composition of module-finite maps, and thus by Remark 1.24 it is also module-finite. □

In what follows, we will need the following elementary linear algebra fact, which is actually very useful in various contexts within commutative algebra. In fact, later in this class we will use this useful fact again, perhaps when you least expect it. This is a nice example of an algebra fact that holds over any ring that we can actually reduce to the case of fields.

Definition 1.33. The **classical adjoint** of an $n \times n$ matrix $B = [b_{ij}]$ is the matrix $\operatorname{adj}(B)$ with entries $\operatorname{adj}(B)_{ij} = (-1)^{i+j} \det(\widehat{B_{ji}})$, where $\widehat{B_{ji}}$ is the matrix obtained from B by deleting its jth row and ith column.

Lemma 1.34 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^n$, and $r \in R$.*

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

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 will 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 $\psi : \mathbb{Z}[X] \twoheadrightarrow R$ be a surjection, $a_{ij} \in \mathbb{Z}[X]$ 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

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

in the case when $R = \mathbb{Z}[X]$, and we can do this entry by entry. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of a field (its fraction field). Since both sides of the equation

$$(\mathrm{adj}(B)B)_{ij} = (\det(B)I_{n\times n})_{ij}$$

live in R and are equal in the fraction field (by linear algebra) they are equal in R. This holds for all i, j, and thus 1) holds.

2) By assumption, we have $(rI_{n\times n} - B)v = 0$, so by part 1)

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

Theorem 1.35 (Module finite implies integral)**.** *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

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

Suppose that $R = Af_1 + \cdots + Af_n$. We may assume that $f_1 = 1$, perhaps by adding a module generator. Since every element in R is an A-linear combination of $f_1, \ldots, f_n$, this is in particular true for the elements $rf_1, \ldots, rf_n$. Thus we can find $a_{ij} \in A$ such that

$$rf_i = \sum_{j=1}^{t} a_{ij} f_j$$

for each i. Consider the matrix $C = [a_{ij}]$ and the column vector $v = (f_1, \ldots, f_n)$. We can now write the equalities above more compactly as $rv = Cv$. By the determinantal trick, $\det(rI_{n\times n} - C)v = 0$. Since we chose one of the entries of v to be 1, we have in particular that $\det(rI_{n\times n} - C) = 0$. Expanding this determinant as a polynomial in r, this is a monic equation with coefficients in A. $\square$

We are now ready to show the following important characterization of module-finite extensions, which tells us exactly what we need besides algebra-finite to force an extension to be module-finite:

Corollary 1.36. *An A-algebra R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): Module-finite implies integral by Theorem 1.35, and algebra-finite by Lemma 1.19. ($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, then each r_i is integral over A, and this implies R is module-finite over A by Proposition 1.32,. □

Corollary 1.37. *If R is generated as an algebra over A by integral elements, then R is integral over A.*

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 $r \in A[L]$. This $A[L]$ is now a finitely-generated algebra generated by integral elements, and thus by Corollary 1.36 it must be module-finite over A. By Theorem 1.35, module-finite implies integral, and thus $A[L]$ is an integral extension of A. In particular, $r \in A[L]$ is integral over A. □

Corollary 1.38. *Given any ring extension $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

Proof. By Corollary 1.37, the A-subalgebra of R generated by all elements in R that are integral over A is integral over A, so it is contained in the set of all elements that are integral over A: this means that

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

so equality holds throughout, and $\{$integral elements$\}$ is a ring. □

In other words, the integral closure of A in R is a subring of R containing A.

Example 1.39.

1) The ring $\mathbb{Z}[\sqrt{d}]$, where $d \in \mathbb{Z}$ is not a perfect square, is integral over $\mathbb{Z}$. Indeed, $\sqrt{d}$ satisfies the monic polynomial $x^2 - d$, and since the integral closure of $\mathbb{Z}$ is a ring containing $\mathbb{Z}$ and $\sqrt{d}$, and $\mathbb{Z}[\sqrt{d}]$ is the smallest such ring, we conclude that every element in $\mathbb{Z}[\sqrt{d}]$ is integral over $\mathbb{Z}$.

2) Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. Then we claim that S is module-finite over R, though to see this we first need to realize R as a subring of S. To do that, consider the $\mathbb{C}$-algebra homomorphism

$$\begin{aligned} R &\xrightarrow{\varphi} S \\ (x, y) &\longmapsto (x, y). \end{aligned}$$

The kernel of φ consists of the polynomials in x and y that are multiples of $x^2 + y^2 + z^2$, but any nonzero multiple of $x^2 + y^2 + z^2$ in $\mathbb{C}[x, y, z] = R[z]$ must have z-degree at least 2, which implies it involves z and thus it is not in $\mathbb{C}[x, y]$. We conclude that φ is injective, and thus $R \subseteq S$.

Now S is generated over R as an algebra by one element, z, and z satisfies the monic equation $t^2 + (x^2 + y^2) = 0$, so S is integral over R.

Note, however, that not all integral extensions are module-finite.

Example 1.40. Let k be a field, and consider the $k[x]$-algebra R given by

$$k[x] \subseteq R = k[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots].$$

Note that $x^{1/n}$ satisfies the monic polynomial $t^n - x$, and thus it is integral over $k[x]$. Since R is generated by elements that are integral over $k[x]$, by Corollary 1.37 it must be an integral extension of A. However, $k[x] \subseteq R$ is not algebra-finite, and thus it is also not module-finite.

Exercise 6. Given ring extensions $A \subseteq B \subseteq C$, the extensions $A \subseteq B$ and $B \subseteq C$ are integral if and only if $A \subseteq C$ is integral.

Finally, here is a useful fact about integral extensions that we will use multiple times.

Theorem 1.41. *If $R \subseteq S$ is an integral extension of domains, then R is a field if and only if S is a field.*

Proof. Suppose that R is a field, and let $s \in S$ be a nonzero element, which is necessarily integral over R. The ring $R[s]$ is algebra-finite over R by construction, and integral over R by Corollary 1.37. Since $R \subseteq R[s]$ is integral and algebra-finite, it must also be module-finite by Corollary 1.36. Since R is a field, this means that $R[s]$ is a finite-dimensional vector space over R. Since $R[s] \subseteq S$ is a domain, the map $R[s] \xrightarrow{s} R[s]$ is injective. Notice that this is a map of finite-dimensional R-vector spaces, and thus it must also be surjective. In particular, there exists an element $t \in R[s]$ such that $st = 1$, and thus s is invertible. We conclude that S must be a field.

Now suppose that S is a field, and let $r \in R$. Since $r \in R \subseteq S$, there exists an inverse r^{-1} for r in S, which must be integral over R. Given any equation of integral dependence for r^{-1} over R, say

$$(r^{-1})^n + a_{n-1}(r^{-1})^{n-1} + \cdots + a_0 = 0$$

with $a_i \in R$, we can multiply by r^{n-1} to obtain

$$r^{-1} = -a_{n-1} - \cdots - a_0 r^{n-1} \in R.$$

Therefore, r is invertible in R, and R is a field. □

Before we move on from algebra-finite and module-finite extensions, we should remark on what the situation looks like over fields. First, note that over a field, module-finite just means finite dimensional vector space. While over a general ring the notions of algebra-finite and module-finite are quite different, they are actually equivalent over a field. This is a very deep fact, and we will unfortunately skip its proof — since it is a key ingredient in proving a fundamental result in algebraic geometry, we will leave it for the algebraic geometry class next semester.

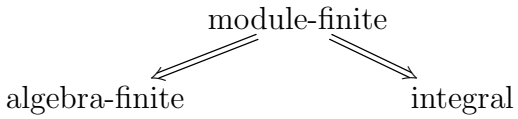
Theorem 1.42 (Zariski's Lemma)**.** *A field extension $k \subseteq L$ is algebra-finite if and only if it is module-finite.*

The following corollary follows immediately from what we proved in this section:

Corollary 1.43. *Let k be an algebraically closed field. If the field extension $k \subseteq L$ is algebra-finite, then $k = L$.*

Proof. By Theorem 1.42, $k \subseteq L$ must be module-finite. By Theorem 1.35, any module-finite extension must be integral. When we are over a field, integral is the same as algebraic, but integrally closed fields have no nontrivial algebraic extensions. □

We have shown the following about ring extensions:



The remaining implications are all false:

- Given an indeterminate x, the extension $R \subseteq R[x]$ is algebra-finite but not module finite nor integral.
- Example 1.40 is an example of an integral extension that is not module-finite nor algebra-finite.

1.5 We interrupt this broadcast for a very short introduction to exact sequences

Homological techniques play a central role in commutative algebra. Ideally, our study of commutative algebra would start with a semester long course on homological algebra; but we are not assuming any homological algebra background, and thus we need to introduce some elementary homological algebra tools.

Definition 1.44. An **exact sequence** of R-modules is a sequence

$$\cdots \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$$

of R-modules and R-module homomorphisms such that $\operatorname{im} f_n = \ker f_{n+1}$ for all n. An exact sequence of the form

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is called a **short exact sequence**.

Example 1.45. Let $R = k[x]/(x^2)$, where k is any field. The $R \xrightarrow{x} R$ has image and kernel (x), so the following is an exact sequence:

$$\cdots \longrightarrow R \xrightarrow{x} R \xrightarrow{x} R \longrightarrow \cdots$$

Remark 1.46. The sequence

$$0 \longrightarrow M \xrightarrow{f} N$$

is exact if and only if f is injective. Similarly,

$$M \xrightarrow{f} N \longrightarrow 0$$

is exact if and only if f is surjective. As a consequence, we see that

$$0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$$

is exact if and only if f is an isomorphism. Moreover,

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is a short exact sequence if and only if

- f is injective
- g is surjective
- $\operatorname{im} f = \ker g$.

So when this is indeed a short exact sequence, we can identify A with its image $f(A)$, which makes $A = \ker g$. Moreover, since g is surjective, by the First Isomorphism Theorem we conclude that $C \cong B/A$, so we might abuse notation and identify C with B/A. In particular, note that $C = \operatorname{coker} f$.

In summary, any short exact sequence encodes an inclusion and its cokernel, or equivalently a surjection an its kernel. To give a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is the same as giving an inclusion of modules $A \subseteq B$ and the corresponding quotient module B/A.

Example 1.47. The following is a short exact sequence of $\mathbb{Z}$-modules:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Indeed, multiplication by 2 on $\mathbb{Z}$ is injective, and its cokernel is $\mathbb{Z}/2\mathbb{Z}$. Another way to look at this is to notice that the kernel of the canonical projection map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the ideal generated by 2, which is a free $\mathbb{Z}$-module with 1 generator. The map $\mathbb{Z} \xrightarrow{2} \mathbb{Z}$ corresponds to the inclusion of that module in $\mathbb{Z}$.

Remark 1.48. Suppose that

$$0 \longrightarrow M \longrightarrow 0$$

is an exact sequence. This means that the image of the zero map to M, which is the zero module, is the same as the kernel of the zero map from M, which is all of M. Thus saying that

$$0 \longrightarrow M \longrightarrow 0$$

is equivalent to saying that $M = 0$.

1.6 Noetherian rings

Most rings that commutative algebraists naturally want to study are noetherian. Noetherian rings are named after Emmy Noether, who is in many ways the mother of modern commutative algebra.

Definition 1.49 (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 1.50. *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, 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, so R is not noetherian.
(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, since (3) is a special case of (1).
(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, so (3) does not hold.
(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 $I = (a_1, \ldots, a_t)$. Now since each a_i is in I, it must be in some I_{n_i}, by definition. Thus for any $N \geqslant \max n_i$, we have $a_1, \ldots, a_t \in I_N$. But then $I_N = I$, and thus $I_n = I_{n+1}$ for all $n \geqslant N$. Thus the original chain stabilizes, and R is noetherian. □

Remark 1.51. When we say that every non-empty family of ideals has a maximal element, that maximal element does not have to be unique in any way. An ideal I is maximal in the family $\mathcal{F}$ if $I \subseteq J$ for some $J \in \mathcal{F}$ implies $I = J$. However, we might have many incomparable maximal elements in $\mathcal{F}$. For example, every element in the family of ideals in $\mathbb{Z}$ given by

$$\mathcal{F} = \{(p) \mid p \text{ is a prime integer}\}$$

is maximal.

Remark 1.52. If R is a noetherian ring and S is a non-empty set of ideals in R, not only does S have a maximal element, but every element in S must be contained in a maximal element of S. Given an element $I \in S$, the subset T of S of ideals in S that contain I is nonempty, and must then contain a maximal element J by Proposition 1.50. If $J \subseteq L$ for some $L \in S$, then $I \subseteq L$, so $L \in T$, and thus by maximality of J in T, we must $J = L$. This proves that J is in fact a maximal element in S, and by construction it contains I.

Example 1.53.

1) If $R = k$ is a field, the only ideals in k are (0) and $(1) = k$, so k is a noetherian ring.

2) $\mathbb{Z}$ is a noetherian ring, since all ideals are principal. 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, $R = k[x_1, x_2, \ldots]$: 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

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

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

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

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!

Lemma 1.54. *Let R be a ring and I an ideal in R. If R is noetherian, then so is R/I.*

Proof. There is an order preserving bijection

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

that sends the ideal $J \supseteq I$ to J/I; its inverse is the map that sends each ideal in R/I to its preimage. Given this bijection, chains of ideals in R/I come from chains of ideals in R that contain J. This implies that if R is noetherian, then R/I is noetherian as well. □

This gives us many more examples of noetherian rings, by simply taking quotients of the examples above. We will soon show that any polynomial ring over a notherian ring is also notherian; as a consequence, we obtain that any quotient of a polynomial ring over a field is noetherian. This is the content of Hilbert's Basis Theorem.

But first, we need to talk about noetherian modules.

Definition 1.55 (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; the proof is analogous, so we leave it as an exercise.

Proposition 1.56 (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.

Remark 1.57. The submodules of a ring are its ideals. Thus a ring R is a noetherian ring if and only if R is noetherian as a module over itself. However, a noetherian ring need not be a noetherian module over a subring. For example, consider $\mathbb{Z} \subseteq \mathbb{Q}$. These are both noetherian *rings*, but $\mathbb{Q}$ is not a noetherian $\mathbb{Z}$-module; for example, the following is an ascending chain of submodules which does not stabilize:

$$0 \subsetneq \frac{1}{2}\mathbb{Z} \subsetneq \frac{1}{2}\mathbb{Z} + \frac{1}{3}\mathbb{Z} \subsetneq \frac{1}{2}\mathbb{Z} + \frac{1}{3}\mathbb{Z} + \frac{1}{5}\mathbb{Z} \subsetneq \cdots .$$

A module B is noetherian if and only if it has a submodule A such that both A and B/A are noetherian.

Lemma 1.58 (Noetherianity in exact sequences)**.** *In an exact sequence of modules*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

B is noetherian if and only if A and C are noetherian.

Proof. Assume B is noetherian. Since A is a submodule of B, and its submodules are also submodules of B, A is noetherian. Moreover, any submodule of B/A is of the form D/A for some submodule $D \supseteq A$ of B. Since every submodule of B is finitely generated, every submodule of C is also finitely generated. Therefore, C is noetherian.

Conversely, assume that A and C are noetherian, and let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be a chain of submodules of B. First, note that

$$M_1 \cap A \subseteq M_2 \cap A \subseteq \cdots$$

is an ascending chain of submodules of A, and thus it stabilizes. Moreover,

$$g(M_1) \subseteq g(M_2) \subseteq g(M_3) \subseteq \cdots$$

is a chain of submodules of C, and thus it also stabilizes. Pick a large enough index n such that both of these chains stabilize. We claim that $M_n = M_{n+1}$, so that the original chain stabilizes as well. To show that, take $x \in M_{n+1}$. Then

$$g(x) \in g(M_{n+1}) = g(M_n)$$

so we can choose some $y \in M_n$ such that $g(x) = g(y)$. Then $x - y \in \ker g = \operatorname{im} f = A$. Now note that $y \in M_n \subseteq M_{n+1}$, so $x - y \in M_{n+1}$, and thus

$$x - y \in M_{n+1} \cap A = M_n \cap A.$$

Then $x - y \in M_n$, and since $y \in M_n$, we must have $x \in M_n$ as well. □

Corollary 1.59. *If A and B are noetherian R-modules, then $A \oplus B$ is a noetherian R-module.*

Proof. Apply the previous lemma to the short exact sequence

$$0 \longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0\,.$$ □

Corollary 1.60. *A module M is noetherian if and only if M^n is noetherian for some n. In particular, if R is a noetherian ring then R^n is a noetherian module.*

Proof. We will do induction on n. The case $n = 1$ is a tautology. For $n > 1$, consider the short exact sequence

$$0 \longrightarrow M^{n-1} \longrightarrow M^n \longrightarrow M \longrightarrow 0$$

Lemma 1.58 and the inductive hypothesis give the desired conclusion. □

Proposition 1.61. *Let R be a noetherian ring. Given an R-module M, M is a noetherian R-module if and only if M is finitely generated. Consequently, 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. Then M is isomorphic to a quotient of R^n for some n, which is noetherian by Corollary 1.60 and Lemma 1.54. □

Remark 1.62. The notherianity hypothesis is important: if R is a non-noetherian ring and M is a finitely generated R-module, M might not be noetherian. For a dramatic example, note that R itself is a finitely generated R-module, but not noetherian.

Now we are ready to prove Hilbert's Basis Theorem. David Hilbert was 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 work, and he later invited her to join the Göttingen Math Department — many of her amazing contributions to algebra happened during her time in Göttingen. Unfortunately, some of the faculty opposed a woman joining the department, and for her first two years in Göttingen, 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.

Theorem 1.63 (Hilbert's Basis Theorem)**.** *If R is a noetherian ring, then the polynomial rings $R[x_1, \dots, x_d]$ and $R[\![x_1, \dots, x_d]\!]$ are Noetherian for any $d \geqslant 1$.*

Proof. We will give the proof for polynomial rings, and at the end we will indicate what the difference is in the argument for the power series ring case. First, note that by induction on d, we can reduce to the case $d = 1$.

Given an ideal $I \subseteq R[x]$, consider the set of leading coefficients of all polynomials in I,

$$J := \{a \in R \mid \text{there is some } ax^n + \text{lower order terms (with respect to } x) \in I\}.$$

We can check (exercise!) that this is an ideal of R. Since R is noetherian, Proposition 1.50 says that J is finitely generated, so let $J = (a_1, \dots, a_t)$. Pick $f_1, \dots, f_t \in R[x]$ such that the leading coefficient of f_i is a_i, and set $N = \max_i\{\deg f_i\}$.

Let $f \in I$. The leading coefficient of f is an R-linear combination of $a_1, \dots, a_t$. If f has degree greater than N, then we can cancel off the leading term of f by subtracting a suitable combination of the f_i. Therefore, any $f \in I$ can be written as $f = g + h$ for some $h \in (f_1, \dots, f_t)$ and $g \in I$ with degree at most N. In particular, note that $g \in I \cap (R + Rx + \cdots + Rx^N)$. Since $I \cap (R + Rx + \cdots + Rx^N)$ is a submodule of the finitely generated free R-module $R + Rx + \cdots + Rx^N$, it must also be finitely generated as an R-module. Given such a generating set, say $I \cap (R + Rx + \cdots + Rx^N) = (f_{t+1}, \dots, f_s)$, we can write any element $f \in I$ as an $R[x]$-linear combination of these generators $f_{t+1}, \dots, f_s$ and the original $f_1, \dots, f_t$. Therefore, $I = (f_1, \dots, f_t, f_{t+1}, \dots, f_s)$ is finitely generated as an ideal in $R[x]$, and $R[x]$ is a Noetherian ring.

In the power series case, take J to be the set of coefficients of *lowest degree* terms. □

Remark 1.64. We can rephrase Hilbert's Basis 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.

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

Corollary 1.65. *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. Any 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 $\mathbb{C}$. We will see more examples of these when we talk about local rings.

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

Theorem 1.66 (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 $C = A[f_1, \dots, f_r]$ and $C = Bg_1 + \cdots + Bg_s$. Then,

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

for some $b_{ij}, b_{ijk} \in B$. Let $B_0 = A[\{b_{ij}, b_{ijk}\}] \subseteq B$. This is a finitely generated A-algebra; by Corollary 1.65, since A is noetherian, so is B_0.

We claim that $C = B_0\, g_1 + \cdots + B_0 g_s$. Given an element $c \in C$, write c as a polynomial expression in $f_1, \dots, f_r$. Since the f_i are linear combinations of the g_i with coefficients in the b_{ij}, we have $c \in A[\{b_{ij}\}][g_1, \dots, g_s]$. Then using the equations for $g_i g_j$ repeatedly, we can rewrite c as a linear combination of the g_i with coefficients in B_0.

Since B_0 is noetherian and C is a finitely generated B_0-module, C is a noetherian B_0-module, by Proposition 1.61. Since $B \subseteq C$, then B is also a finitely generated B_0-module. In particular, $B_0 \subseteq B$ is algebra-finite. Since $A \subseteq B_0$ is algebra-finite, we conclude that $A \subseteq B$ is algebra-finite, as required. □

1.7 An application to invariant rings

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

Question 1.67. Given a (finite) set of symmetries, consider the collection of polynomial functions that are fixed by all of those symmetries. Can we describe all the fixed polynomials in terms of finitely many of them?

To make this precise, let G be a group acting on a ring R. The main case we have in mind is when $R = k[x_1, \ldots, x_d]$ and k is a field; we let G act trivially on k, and the action respects the sum and product in the ring:

$$g \cdot \left(\sum_a c_a x_1^{a_1} \cdots x_d^{a_d} \right) = \sum_a c_a (g \cdot x_1)^{a_1} \cdots (g \cdot x_d)^{a_d}.$$

We are interested in the set of elements that are **invariant** under the action,

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

Note that R^G is a subring of R. Indeed, given $r, s \in R^G$, then

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

since each g is a homomorphism. Note also that if $G = \langle g_1, \ldots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \ldots, t$. The question above can now be rephrased as follows:

Question 1.68. Given a finite group G acting on $R = k[x_1, \ldots, x_d]$, is R^G a finitely generated k-algebra?

Note that R^G is a k-subalgebra of R. Even though R is a finitely generated k-algebra, this does not guarantee a priori that R^G is a finitely generated k-algebra — recall Example 1.23, where we saw a subalgebra of a finitely generated algebra which is nevertheless not finitely generated.

Example 1.69. Consider the group with two elements $G = \{e, g\}$. To define an action of G on $R = k[x]$, we need only to define $g \cdot x$, since e is the identity and g acts linearly. Consider the action of G on $R = k[x]$ given by $g \cdot x = -x$, so $g \cdot f(x) = f(-x)$. Suppose that the characteristic of k is not 2, so $-1 \neq 1$. Write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. We have $g \cdot x^i = (-x)^i = (-1)^i x^i$, so

$$g \cdot f = (-1)^n a_n x^n + (-1)^{n-1} a_{n-1} x^{n-1} + \cdots + a_0,$$

which differs from f unless for each odd i, $a_i = 0$. That is,

$$R^G = \{f \in R \mid \text{every term of } f \text{ has even degree}\}.$$

Any such f is a polynomial in x^2, so we have

$$R^G = k[x^2].$$

In particular, R^G is a finitely generated k-algebra.

Exercise 7. Generalize the last example as follows: let k be a field with a primitive dth root of unity ζ, and let $G = \langle g \rangle \cong C_d$ act on $R = k[x_1, \ldots, x_n]$ via $g \cdot x_i = \zeta x_i$ for all i. Then

$$R^G = \{f \in R \mid \text{every term of } f \text{ has degree a multiple of } d\} = k[\{\text{monomials of degree d}\}].$$

This what is known as the Veronese subring of R of degree d.

Example 1.70 (Standard representation of the symmetric group)**.** Let S_n be the symmetric group on n letters acting on $R = k[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$. For example, if $n = 3$, then $f = x_1^2 + x_2^2 + x_3^2$ is invariant, while $g = x_1^2 + x_1x_2 + x_2^2 + x_3^2$ is not, since swapping 1 with 3 gives a different polynomial.

You may recall the Fundamental Theorem of Symmetric Polynomials says that every element of R^{S_n} can be written as polynomial expression in the elementary symmetric polynomials

$$\begin{aligned} e_1 &= x_1 + \cdots + x_n \\ e_2 &= \sum x_i x_j \\ &\vdots \\ e_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

More precisely, $R^{S_n} = k[e_1, \ldots, e_n]$. For example, f above is $e_1^2 - 2e_2$. In fact, any symmetric polynomial can be written like so in a *unique* way, so R^{S_n} is a free k-algebra. So even though we have infinitely many invariant polynomials, we can understand them in terms of only finitely many of them, which are *fundamental* invariants.

Proposition 1.71. *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. By Corollary 1.36, integral and algebra-finite implies module-finite, so we will show that R is algebra-finite and integral over R^G.

First, since $k \subseteq R^G$ and R is generated finitely generated k-algebra, it is generated by the same finite set as an R^G-algebra as well. Thus $R^G \subseteq R$ is algebra-finite.

To show that $R^G \subseteq R$ is integral, let us first extend the action of G on R to $R[t]$ trivially, meaning that we will let G fix t. Given $r \in R$, consider the polynomial

$$F_r(t) := \prod_{g \in G} (t - g \cdot r) \in R[t].$$

Now G fixes $F_r(t)$, since for each $h \in G$,

$$h \cdot F_r(t) = h \prod_{g \in G} (t - g \cdot r) = \prod_{g \in G} (h \cdot t - (hg) \cdot r) = F_r(t)$$

Thus, $F_r(t) \in (R[t])^G$. Notice that $(R[t])^G = R^G[t]$, since

$$g(a_n t^n + \cdots + a_0) = a_n t^n + \cdots + a_0 \implies (g \cdot a_n)t^n + \cdots + (g \cdot a_0) = a_n t^n + \cdots + a_0.$$

Therefore, $F_r(t) \in R^G[t]$. The leading term (with respect to t) of $F_r(t)$ is $t^{|G|}$, so $F_r(t)$ is monic. On the other hand, one of the factors of $F_r(t)$ is $(t - r)$, so $F_r(r) = 0$. Therefore, r satisfies a monic polynomial with coefficients in R^G, and thus R is integral over R^G. $\square$

Theorem 1.72 (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. The desired result is now a corollary of the Artin-Tate Lemma. □

Chapter summary

- R is a Noetherian ring $\iff$ every ideal I in R is Noetherian
- M is a Noetherian R-module $\underset{R \text{ Noeth}}{\overset{\text{general}}{\rightleftharpoons}}$ M is a finitely generated R-module

$A \subseteq R$ extension of rings:

- $A \subseteq R$ module-finite $\iff$ $R = Af_1 + \cdots + Af_n$ for some $f_i \in R$ $\iff$ $R \cong A^n/N$, $N \subseteq A^n$ submod
- $A \subseteq R$ algebra-finite $\iff$ $R = A[f_1, \ldots, f_n]$ for some $f_i \in R$ $\iff$ $R \cong A[x_1, \ldots, x_i]/I$, x_i indeterminates
  - $A \subseteq R$ algebra-finite $\iff$ $R = A[f_1, \ldots, f_n]$, $f_i \in R$
  - $A \subseteq R$ algebra-finite, A Noetherian $\implies$ R Noetherian ring
  - $A \subseteq R$ module-finite $\iff$ $\begin{cases} \text{algebra-finite} & \not\Longrightarrow \\ \text{and integral} & \not\Longrightarrow \end{cases}$ module-finite

Artin-Tate Lemma: $\underbrace{A \subseteq \underbrace{B \subseteq C}_{\text{mod-fin}}}_{\text{alg-fin}}$ (A Noeth)

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.

We can now do all sorts of computations over our ring R. For example, we can define an ideal in R, as follows:

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

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

o3 : Ideal of R
```

Above we have set I to be the ideal in R that is generated by x^2, y^2, xy. The notation `ideal( )` requires the usage of `^` for powers and $*$ for products; alternatively, we can define the exact same ideal with the notation `ideal" "`, as follows:

```
i3 : I = ideal"x2,y2,xy"

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

o3 : Ideal of R
```

Now we can use this ideal I to either define a quotient ring $S = R/I$ or the R-module $M = R/I$, as follows:

```
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 map

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

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 R`.

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 second 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:

```
i6 : U = k[a,b,c]

o6 = U

o6 : PolynomialRing

i7 : f = map(R,U,{x^2,x*y,y^2})
                 2        2
o7 = map(R,U,{x , x*y, y })

o7 : RingMap R <--- U

i8 : J = ker f
             2
o8 = ideal(b  - a*c)

o8 : Ideal of U

i9 : T = U/J

o9 = T

o9 : QuotientRing
```

Our ring T at the end is isomorphic to the 2nd Veronese of R, which is the ring we wanted. Note the syntax order in `map`: first target, then source, then a list with the images of each algebra generator.

A.2 Asking Macaulay2 for help

As you're learning how to use Macaulay2, you will often find yourself needing some help. Luckily, Macaulay2 can help you directly! For example, suppose you know the name of a command, but do not remember the syntax to use it. You can ask `?command`, and Macaulay2 will show you the different usages of the command you want to know about.

```
i10 : ?primaryDecomposition

primaryDecomposition -- irredundant primary decomposition of an ideal

  * Usage:
        primaryDecomposition I
  * Inputs:
      * I, an ideal, in a (quotient of a) polynomial ring R
  * Optional inputs:
      * MinimalGenerators => a Boolean value, default value true, if false, the
        components will not be minimalized
      * Strategy => ..., default value null,
  * Outputs:
      * a list, containing a minimal list of primary ideals whose intersection
        is I

Ways to use primaryDecomposition :
==================================

  * "primaryDecomposition(Ideal)" -- see "primaryDecomposition" -- irredundant
    primary decomposition of an ideal
  * "primaryDecomposition(Module)" -- irredundant primary decomposition of a
    module
  * "primaryDecomposition(Ring)" -- see "primaryDecomposition(Module)" --
    irredundant primary decomposition of a module

For the programmer
==================

The object "primaryDecomposition" is a method function with options.
```

If instead you'd rather read the complete Macaulay2 documentation on the command you are interested in, you can use the `viewHelp` command, which will open an html page with the documentation you asked for. So running

```
i11 : viewHelp "primaryDecomposition"
```

will open an html page dedicate to the method `primaryDecomposition`, which includes examples and links to related methods.

A.3 Basic commands

Many Macaulay2 commands are easy to guess, and named exactly what you would expect them to be named. Often, googling "Macaulay2" followed by a few descriptive words will easily land you on the documentation for whatever you are trying to do.

Here are some basic commands you will likely use:

- `ideal`$(f_1, \ldots, f_n)$ will return the ideal generated by $f_1, \ldots, f_n$. Here products should be indicated by $*$, and powers with $\widehat{}$. If you'd rather not use $\widehat{}$ (this might be nice if you have lots of powers), you can write `ideal`$(f_1, \ldots, f_n)$ instead.
- `map`$(S, R, f_1, \ldots, f_n)$ gives a ring map $R \to S$ if R and S are rings, and R is a quotient of $k[x_1, \ldots, x_n]$. The resulting ring map will send $x_i \mapsto f_i$. There are many variations of `map` — for example, you can use it to define R-module homomorphisms — but you should carefully input the information in the required format. Try `viewHelp map` in Macaulay2 for more details
- `ker`(f) returns the kernel of the map f.
- `I + J` and `I*J` return the sum and product of the ideals I and J, respectively.
- `A = matrix`$\{\{a_{1,1}, \ldots, a_{1,n}\}, \ldots, \{a_{m,1}, \ldots, a_{m,n}\}\}$ returns the matrix

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ & \ddots & \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}$$

If you are familiar with any other programming language, many of the basics are still the same. For example, some of the commands we will use return lists, and we might often need to do operations on lists. As with many other programming languages, a list is indicated by { } with the elements separated by commas.

```
i6 : w = {ZZ, 3, ideal"xy3"}
                          3
o6 = {ZZ, 3, ideal(x*y )}

o6 : List
```

As in most programming languages, Macaulay2 follows the convention that the first position in a list is the 0th position.

The method `primaryDecomposition` returns a list of primary ideals whose intersection is the input ideal, and `associatedPrimes` returns the list of associated primes of the given ideal or module. Operations on lists are often intuitive. For example, let's say we want to find the primary component of an ideal with a particular radical.

```
i1 : R = QQ[x,y];

i2 : I = ideal"x2,xy";

o2 : Ideal of R

i3 : prim = primaryDecomposition I
                            2
o3 = {ideal x, ideal (y, x )}

o3 : List

i4 : L = select(prim, Q -> radical(Q) == ideal"x,y")
                  2
o4 = {ideal (y, x )}

o4 : List
```

The method `select` returns a list of all the elements in our list with the required properties. In this case, if we actually want the primary ideal we just selected, as opposed to a list containing it, we need to extract the first component of our list L.

```
i5 : L_0
                 2
o5 = ideal (y, x )

o5 : Ideal of R
```

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.