Commutative Algebra

Yankı Lekili

■ Statement of a convention used throughout the text.
► Little facts that can be checked but we don't bother to check explicitly. If you don't find what's stated intuitive, you should stop and think about how to prove it. If you can't, then consult a book and if that doesn't help either, please come ask me. I will assume that you know how to prove these.
◁ Exercise. Try it!
□ Marks the end of a proof.

When something is defined for the first time, I make it **bold** and when I want to emphasise something I underline it.

`Code snippets in Macaulay 2 are inserted with this font.`
`I won't ask you any coding problems in the exam but you should install Macaulay 2 in your computer and have fun with it as you learn commutative algebra.`
`Macaulay 2 is available at`

`https://faculty.math.illinois.edu/Macaulay2/`.

`It is available for basically all platforms.`
`I run it on a GNU-Linux machine where you just type M2 to run it on the command line.`

☡ These are fresh notes that I typed up recently. I expect that there are lots of typos. If you detect them, please send me an email and then come to the office hour to collect your triple chocolate cookie.

$:=$ denotes a definition. $\simeq$ denotes an isomorphism. I very often make a mistake and use $=$ where I really meant to use $:=$ or $\simeq$. No cookies for that!

1 Prelude

Commutative Algebra has its roots in Algebraic Number Theory and forms the foundation of the modern theory of Algebraic Geometry.

In this course, the students will learn about Noetherian rings and modules, Hilbert basis theorem, Hilbert polynomials, Gröbner basis and Buchberger's algorithm, integral dependence, Noether normalization, the Nullstellensatz, Spectrum of rings and Zariski topology, localisation, Artin rings, dimension theory, Krull's principal ideal theorem, Cohen-Seidenberg lying over/going up theorem.

1.1 Algebraic Geometry

Algebraic Geometry is the study of algebraic varieties - spaces cut out by polynomial equations in several variables. An example of an algebraic variety is the subspace of k^2 cut out by the equation $X^2 = Y^3$ where k is a field. The algebraic functions on these spaces are commutative algebras isomorphic to subquotients of polynomial rings in several variables. For example, the functions on the space cut out by $X^2 = Y^3$ is given by the quotient ring $k[X, Y]/(X^2 - Y^3)$. Hilbert's Nullstellensatz, one of the main themes in this course, gives a dictionary between the geometry of algebraic varieties and the algebra of functions on these spaces. In a sense, there is a complete correspondence: problems of algebra can be turned into geometry and vice versa.

1.2 Algebraic Number Theory

Algebraic Number Theory is a subject which was developed with the main goal of solving Fermat's Last Theorem which states that there are no integer solutions to $X^n + Y^n = Z^n$ for $n > 2$. An early approach to this question was by making use of the factorisation

$$Y^n = \prod_{i=0}^{n} (Z - \xi^i X) \text{ with } \xi^n = 1$$

in the commutative ring $\mathbb{Z}[\xi]$. If one knows that every element of $\mathbb{Z}[\xi]$ can be factorised into primes (like the case of $\mathbb{Z}$) by using elementary methods in divisibility one arrives at a contradiction. Thus, it is of importance to understand whether such unique factorization property holds. (It turns out this depends on the value of n). Algebraic number theory brings in methods of commutative algebra to approach this problem by studying "number rings" like $\mathbb{Z}[\xi]$ using methods from commutative algebra (and often inspired by analogous geometric results valid for co-ordinate rings of algebraic varieties.)

1.3 Logic: Constructive vs. Non-constructive

"Das ist nicht Mathematik, das ist Theologie."[1] is a famous quote attributed to Paul Gordan, a well-known algebraist in 19^{th} century, about young Hilbert who vastly generalised Gordan's work by proving what is now known as the Hilbert basis theorem and the Nullstellensatz. The proof that Hilbert gave was non-constructive. In modern language, his arguments proved existence results based on axiomatic methods without actually giving an algorithm to construct the desired structure. Hilbert's ideas were revolutionary. The axiomatic methods favors abstract, non-constructive arguments. They tend to be considerably shorter and more elegant. Emmy Noether, a student of Gordan developed this approach significantly and developed what's known as the Noetherian induction. In essence, the non-constructive methods of Hilbert and Noether invoke a version of Axiom of Choice or equivalently Zorn's lemma. Most of modern commutative algebra textbooks accept this axiom and build the theory that way. In more recent years, the advent of computers prompted a renewed interest in constructive methods. The computers vastly increased the scope of computations. The main crux of constructive methods are Gröbner bases and Buchberger's algorithm which simultaneously generalise Gaussian elimination in linear

[1] "This is not mathematics, it is theology."

algebra and the Euclid's division algorithm in the theory of polynomials in one variable to the case study of polynomials in several variables. In this course, we will favour constructive methods when this doesn't take us too far afield. Notably, we will give a proof of Hilbert's Nullstellensatz that is constructive. We will also make use of non-constructive methods when either this is illuminating or else the corresponding constructive argument is much harder. We will not define what constructive or non-constructive means precisely. However, we will specify whenever an argument is non-constructive and hoping that the reader will build an intuitive understanding of these concepts.[2]

2 Rings, Ideals and Modules

This section is mostly basic definitions that layout the protagonists of our topic. Please bear with it as we need these. The fun starts in the next section.

2.1 Rings

Rings are things where you can do addition and multiplication in a compatible way modeled on the ring of integers $\mathbb{Z}$. A general ring does not have to be commutative. For example, the set of 2-by-2 matrices $M_{2,2}(\mathbb{Z})$ is a ring under the familiar addition and multiplication rules but it is not commutative. There are matrices such that $A \cdot B \neq B \cdot A$.

The crucial assumption in this lecture course is the assumption of commutativity of the multiplication.

A **commutative ring with identity** is a set $(R, +, \cdot, 0, 1)$ such that

$$\begin{aligned}
(R, +, 0) &\text{ is an abelian group.} \\
a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\
a \cdot (b + c) &= a \cdot b + a \cdot c. \\
a \cdot b &= b \cdot a \\
a \cdot 1 &= 1 \cdot a = 1.
\end{aligned}$$

Note that a **field** is a commutative ring where every non-zero element a is invertible; i.e., has a multiplicative inverse b such that $ab = 1$. Therefore, any field is a commutative ring. Recall also that an **integral domain** is a subring of a field.

▶ Let R be a ring in which there are no zero divisor, that is, for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$. This is equivalent to R being an integral domain. Indeed, every such ring can be embedded in a field $Frac(R)$ called the **field of fractions** of R consisting only of elements a/b with $a, b \in R$ and $b \neq 0$, which is unique up to isomorphism.

Those elements of a commutative ring R which are invertible are called **units** of the ring R.

[2] Personally, I do not object to nonconstructive proofs depending on Axiom of Choice however I feel that theorems which do not depend o n them are more fundamental.

■ In this course, a ring will always mean a commutative ring with identity.

A **homomorphism** of rings $f : R \to S$ is a map satisfying

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \\ f(1) &= 1 \end{aligned}$$

An integral domain is a **unique factorisation domain (UFD)** if every element a factors as a product of irreducible elements p_i and a unit u: $a = up_1p_2 \dots p_n$ and this representation is unique.

An integral domain R is a **Euclidean domain** if it has a norm $|\cdot| : R \to \mathbb{N}$ such that given a, b with $b \neq 0$, we can find r, q such that $a = bq + r$ and $|r| < |b|$.

2.2 Ideals

Unique factorization domain property does not hold in other rings of integers, such as $\mathbb{Z}[\sqrt{-5}]$, the extension ring obtained by adjoining $\sqrt{-5}$ to $\mathbb{Z}$. We have

$$21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

Theory of ideals ("ideal numbers") was motivated by a desire to restore the property of unique factorization in number fields. The theory of ideals is also motivated via Algebraic Geometry: We will see later that ideals $I(S)$ in the ring of polynomials $\mathbb{C}[X_1, X_2, \dots, X_n]$ are associated to the set of polynomials vanishing along a subset S in the affine space $\mathbb{C}^n$.

Ideal of a ring R is a kernel of a homomorphism $f : R \to S$. Equivalently, an **ideal** is a subset of R that can be characterized by the following properties

$$a, b \in I, a \pm b \in I$$

$$ar \in I, \text{ for } a \in I, r \in R$$

Given an $I \in R$, we can produce a ring R/I with the multiplication $(x + I)(y + I)$ defined to be $xy + I$. There is a natural surjective homomorphism $f : R \to R/I$ sending x to $x + I$ such that $I = \text{Ker}(f)$.

▶ There is a natural bijection between the ideals $J \subset R$ such that $I \subset J$ and the ideals of R/I. Just send J to $f(J)$.

▶ An ideal I in a commutative ring R itself is a commutative ring but without an identity!

Given a subset S of R, the ideal generated by S is the subset

$$(S) = \{r_1s_1 + \dots + r_ts_t | r_i \in R, s_i \in S, t \in \mathbb{N}\}.$$

We write $(f_1, f_2, \dots, f_t)$ for the ideal generated by a finite set of elements $f_1, \dots, f_t \in R$.

■ R itself is the ideal (1) of R. To exclude this ideal, we say that I is a **proper** ideal if I is an ideal of R but not equal to (1).

An ideal is **principal** if it is generated by a single element. A ring is a **principal ideal domain (PID)** if every ideal is principal.

▶ Euclidean domain implies PID.
▶ PID implies UFD (this uses Axiom of Choice).

A ring is called **Noetherian** if all of its ideals are finitely generated. We will study this condition in detail later on. In particular, we will see that most rings of interest in this course are Noetherian, but not all!

◁ Show that the ring of differentiable functions on $\mathbb{R}^n$ is not Noetherian. For the geometry of manifolds, Commutative Algebra is not enough; you need Calculus.

We can define basic operations of addition and multiplication for ideals.

$$I + J = \{a + b | a \in I, b \in J\}$$
$$IJ = \{\sum_{i=1}^{t} a_i b_i | a_i \in I, b_i \in J, t \in \mathbb{N}\}.$$

Multiplication of ideals is commutative: $IJ = JI$ and associative $I(JK) = (IJ)K$. We say that an ideal I divides an ideal K if there exists an ideal J such that $IJ = K$.

▶ The set of ideals of a ring itself is a multiplicative semigroup but is not a ring! There is no additive inverse.

▶ $I \cap J$ is also an ideal. In general, $IJ \subset I \cap J$.

◁ If $I = (m)$, $J = (n)$ in $\mathbb{Z}$, then $IJ = (mn)$, $I \cap J = (\text{lcm}(m, n))$ and $I + J = (\gcd(m, n))$.

Proposition 2.1. *Suppose that the ideals I, J of a ring R are* **coprime***, that is $I + J = R$, then $IJ = I \cap J$.*

Proof. $IJ \subset I \cap J$ by definition. To see the opposite inclusion, since $I + J = R$, we have $I \cap J = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ$. □

Corollary 2.2. *Suppose I, J are coprime ideals in R, then $R/IJ \simeq R/I \times R/J$.*

Proof. It suffices to see that the natural injective map $\pi : R/IJ = R/I \cap J \to R/I \times R/J$ is surjective. Taking $x \in I$ and $y \in J$ such that $x + y = 1$, we have $bx + ay = a \in R/I$ and $bx + ay = b \in R/J$ for any $a, b \in R$ giving surjectivity. □

By induction, we get the following theorem (known as the Sunzi remainder theorem when $R = \mathbb{Z}$).

Theorem 2.3. *Suppose $I_1, I_2, \ldots, I_r$ are pairwise coprime ideals, that is, $I_i + I_j = R$ for $i \neq j$, then $I_1 I_2 \ldots I_r = I_1 \cap I_2 \cap \ldots \cap I_r$ and*

$$R/I_1 \cap I_2 \ldots \cap I_r \simeq R/I_1 \times R/I_2 \times \ldots \times R/I_r.$$

▶ There is also a quotient operation for ideals: $I : J \coloneqq \{a \in R : aJ \subset I\}$. and the saturation $I : J^\infty \coloneqq \{a \in R : aJ^n \subset I \text{ for some } n\}$.

◁ Check that $I : J$ and $I : J^\infty$ are ideals.

2.2.1 maximal, prime and $\sqrt{r}$adical ideals

Clearly, every ideal contains the (0) ideal and is contained in the biggest ideal $(1) = R$.

A **maximal ideal** of a ring R is an ideal $\mathfrak{m}$ such that $\mathfrak{m} \subset I$ implies $\mathfrak{m} = I$ or $I = R$.

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

The next proposition is an application of Zorn's lemma which we recall first.

Zorn's lemma. Let $\mathcal{M}$ be a partially ordered set such that every totally ordered set $\mathcal{T} \subset \mathcal{M}$ has an upper bound, that is an element $b \in \mathcal{M}$ such that $t \leq b$ for all $t \in \mathcal{T}$. Then $\mathcal{M}$ has a maximal element $m \in \mathcal{M}$ such that if $x \in \mathcal{M}$ and $x \geq m$, then $x = m$.

Zorn's lemma is equivalent to the Axiom of Choice.

Proposition 2.4. *If I is a proper ideal, then there exists at least one maximal ideal containing I.*

Proof. Given a proper ideal I in R, let $\mathcal{M}$ be the set of ideals containing I and not containing R. We can order elements of $\mathcal{M}$ by inclusion. Then Zorn's lemma can be applied to $\mathcal{M}$. Indeed, $I \in \mathcal{M}$ so $\mathcal{M}$ is non-empty, and if $\mathcal{T} \subset \mathcal{M}$ is a totally ordered subset, then the union of all the ideals belonging to $\mathcal{T}$ is an ideal of R and belongs to $\mathcal{M}$, so is the lowest upper bound of $\mathcal{T}$. Thus, by Zorn's lemma $\mathcal{M}$ has a maximal ideal. □

In fact, the assertion that every commutative unital ring has a maximal ideal is equivalent to the Axiom of Choice. I don't know how you feel about the Axiom of Choice. As one would expect, for the rings of main interest there are constructive ways of proving the above proposition (and so one doesn't really need to appeal to AC).

The main idea of algebraic geometry is that a commutative ring R is the space of functions on a space (an algebraic variety). The maximal ideals of R then correspond to geometric points of this space. For example, in the ring $R = \mathbb{C}[X, Y]$ the maximal ideals are $\mathfrak{m}_{a,b} = (X - a, Y - b)$, $(a, b) \in \mathbb{C}^2$. Indeed, this is the kernel of the evaluation homomorphism $\mathbb{C}[X, Y] \to \mathbb{C}$ sending a polynomial f to its value $f(a, b)$. So, the points (a, b) of the space $\mathbb{C}^2$ corresponds to the maximal ideals $\mathfrak{m}_{a,b}$ of the polynomial functions $\mathbb{C}[X, Y]$ on this space.

We will prove later in the course ("Nullstellensatz") that there are no other maximal ideals in the polynomial ring $\mathbb{C}[X, Y]$ other than $\mathfrak{m}_{a,b}$ with $(a, b) \in \mathbb{C}^2$.

If $f : R_1 \to R_2$ is a ring map and $\mathfrak{m}$ is a maximal ideal of R_2 then it need not be the case that $f^{-1}(\mathfrak{m})$ is a maximal ideal. For example, consider the inclusion $f : \mathbb{Z} \to \mathbb{Q}$ and observe that $f^{-1}((0)) = (0)$ is not maximal.

A proper ideal I in R is a **prime ideal** if whenever $xy \in I$, then $x \in I$ or $y \in I$.

▶ An ideal I is prime if and only if R/I is an integral domain.

In particular, a maximal ideal is prime.

Proposition 2.5. *If $f : R_1 \to R_2$ is a ring homomorphism and $\mathfrak{p} \subset R_2$ is a prime ideal, then $f^{-1}(\mathfrak{p})$ is a prime ideal.*

Proof. Suppose $xy \in f^{-1}(I)$, then $f(xy) = f(x)f(y) \in I$. Hence, $f(x)$ or $f(y)$ is in I since I is prime. So, x or y is in $f^{-1}(I)$. □

▶ A positive integer n is a prime number if and only if (n) is a prime ideal in $\mathbb{Z}$.

Of course, since any maximal ideal is a prime ideal, the existence proof that we have given for maximal ideals imply that there are many prime ideals. However, we can be a bit more precise as in the following proposition.

A subset S of a ring is called a **multiplicative set** if

$$1 \in S, \text{ and } a, b \in S \implies ab \in S$$

(The difference from a subring is that we do not ask that S is closed under addition.)

Proposition 2.6. *(Krull's lemma) Let R be a ring and $S \subset R$ be a multiplicative set, and I is an ideal of R disjoint from S. Then, there exists a prime ideal $\mathfrak{p}$ of R containing I and is disjoint from S.*

Proof. Applying Zorn's lemma, we can see as before that the set of ideals containing I and disjoint from S has a maximal element. We claim that this maximal element $\mathfrak{p}$ is a prime ideal. Suppose x and y are not in $\mathfrak{p}$. Then the ideals $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ both meet S, hence the ideal $(\mathfrak{p} + (x))(\mathfrak{p} + (y))$ also meet S. On the other hand, $(\mathfrak{p} + (x))(\mathfrak{p} + (y)) \subset \mathfrak{p} + (xy)$. Hence, $xy \notin \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime. □

Let I be an ideal in R, we define **radical** of I to be the ideal

$$\sqrt{I} = \{r \in R | r^n \in I \text{ for some } n > 0\}$$

Such an ideal is called a **radical ideal**.

◁ Show that $\sqrt{I}$ is an ideal. (Use that if $x^n \in I$ and $y^m \in I$ for some $n, m > 0$, then

$$(x + y)^{n+m-1} = \sum_{i+j=n+m-1} r_{i,j} x^i y^j, \quad r_{i,j} \in R$$

is also in I, as in the summands either $i \geq n$ or $j \geq m$.)

Proposition 2.7. $\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$.

Proof. If $\mathfrak{p}$ is a prime ideal containing I, then $x^n \in I \subset \mathfrak{p}$ implies $x \in \mathfrak{p}$ hence $\sqrt{I} \subset \mathfrak{p}$. Conversely, if $x \notin \sqrt{I}$, then consider the multiplicative set $S = \{1, x, x^2, \ldots\}$. By the previous proposition, there exists a prime ideal containing I and not containing x. □

In particular, if we take $I = (0)$ in the previous proposition, we see that

$$\sqrt{(0)} = \{r \in R | r^n = 0 \text{ for some } n > 0\}$$

is the intersection of all prime ideals of R. This is called the **nilradical** and is denoted $\mathcal{N}(R)$. The elements of the nilradical are called the **nilpotent** elements.

The intersection of all maximal ideals of a ring R is called the **Jacobson radical** of R and is denoted $\mathcal{J}(R)$.

◁ Show that $x \in \mathcal{J}(R)$ if and only if $1 - xy$ is a unit of R for all $y \in R$ (uses Zorn's lemma via Proposition 2.4).

◁ Show that $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

◁ Show that a maximal ideal is a prime ideal and a prime ideal is a radical ideal.

◁ Show that if a prime ideal $\mathfrak{p} = I \cap J$ for ideals I and J, then $\mathfrak{p} = I$ or $\mathfrak{p} = J$.

An important class of rings is given by the following.

Definition 2.8. *A ring R is called a* **local ring** *if it has a unique maximal ideal $\mathfrak{m}$.*

▶ In a local ring R, the unique maximal ideal $\mathfrak{m}$ coincides with the Jacobson radical of R.

◁ Show that in a local ring R, the units in R are precisely the elements in $R - \mathfrak{m}$. (uses Zorn's lemma via Proposition 2.4); conversely, a ring R whose non-units form an ideal is a local ring.

2.3 Modules

A **module** M over R is defined by a map $R \times M \to M$, $(r, m) \to rm$ which satisfies:

$$(r_1 r_2)m = r_1(r_2 m)$$

$$(r_1 + r_2)m = r_1 m + r_2 m$$

$$r(m_1 + m_2) = rm_1 + rm_2$$

$$1m = m$$

In other words, it is an abelian on which R acts linearly. If $R = \mathbb{Z}$, then an R-module is the same thing as an abelian group. If R is a field k, then an R-module is a k-vector space. R is a module over itself. A submodule $N \subset M$ of a module M is an R-module N which is also

subgroup of M. A submodule of a ring R is just the same thing as an ideal in that ring. Given an ideal I, we can also consider R/I as an R-module. We can recover the ideal via the annihilator construction

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

The modules of the form R/I are called **cyclic** modules. They have the property that they can be generated by a single element, that is, there exists $x \in M$ such that $M = R \cdot x$.

More generally, we say that an R-module M is **finitely generated** (as a module) if there exist finitely many elements $x_1, \ldots, x_m \in M$ such that $M = R \cdot x_1 + R \cdot x_2 + \ldots + R \cdot x_m$.

$\lhd$ Show that if $M = R \cdot x$ is a cyclic module, then M is isomorphic as an R-module to a module of the form $R/\mathrm{ann}(M)$.

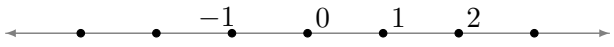
3 Examples

Let's have some examples to play with.

■ k will always denote a field.

There are two main classes of rings that are of interest. Polynomial rings (and their quotients) with field coefficients and rings of integers of algebraic number fields (finite ring extensions of $\mathbb{Z}$). The former class may be referred as "geometric " as it relates to Algebraic Geometry and the latter class may be referred as "arithmetic" as it related to Number Theory.

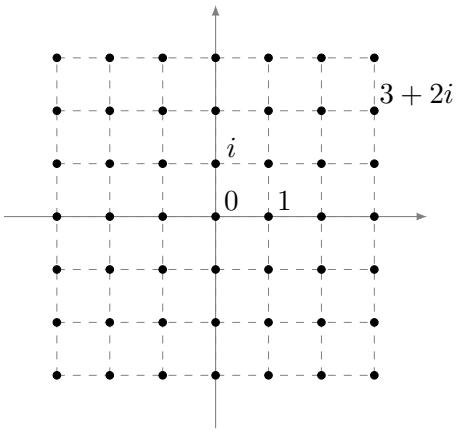
The most fundamental ring is $\mathbb{Z}$ which you encountered in nursery. Prime ideals of $\mathbb{Z}$ are (p) for p prime number and (0).



The polynomial ring in one variable $k[X]$ which you encountered in school is also fundamental. The prime ideals are (f) for f an irreducible polynomial and (0). If k is algebraically closed, then the only irreducible polynomials are $X - \lambda$, $\lambda \in k$.

Both $\mathbb{Z}$ and $k[X]$ are Euclidean domains, hence PID, and so UFD.

The most fundamental quadratic extension is the ring of Gaussian integers $\mathbb{Z}[i]$. We can draw a picture of it as follows:



◁ Show that $\mathbb{Z}[i]$ is an Euclidean domain using the norm $|a+bi| = a^2+b^2$. (Use the fact that disks of unit norm centred at Gaussian integers cover all of the complex plane.)

◁ Show that (a) and (ai) for $a \in \mathbb{Z}$ are prime ideals if only if a is prime number of the form $4n+3$. $(a+bi)$ with $a, b \neq 0$ is a prime ideal if and only if a^2+b^2 is a prime number.

The Eisenstein integers $\mathbb{Z}[\omega]$ with $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{3}i}{2}$ and its subring $\mathbb{Z}[-\sqrt{3}]$ are also good examples to know (note that $\mathbb{Z}[-\sqrt{3}]$ is not a UFD but $\mathbb{Z}[\omega]$ is.).

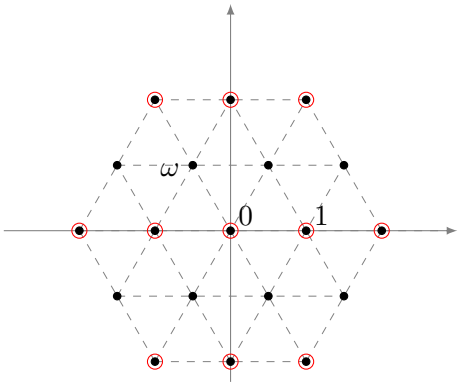


Figure 1: The elements of the ring $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$. The subring $\mathbb{Z}[\sqrt{-3}]$ is marked red.

◁ Show that the Eisenstein integers $\mathbb{Z}[\omega]$ with norm $|a+b\omega| = a^2 - ab + b^2$ is an Euclidean domain.

◁ Show that the ideal $I = (2, 1+\sqrt{-3})$ is not principal in the ring $\mathbb{Z}[\sqrt{-3}]$. (Use that the norm given by $|a+b\sqrt{-3}| = a^2+3b^2$ is multiplicative.)

◁ Show that the ideal $I = (2, 1+\sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ satisfies $I^2 = (2) \cdot I$, hence in $\mathbb{Z}[\sqrt{-3}]$, the ideals do not factor uniquely into prime ideals.

Let R be a ring. The **polynomial ring** with coefficients in R is the set

$$R[X] = \{a_0 + a_1 X + \cdots + a_n X^n | a_i \in R,\ n \in \mathbb{Z}_{\geq 0}\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i\geq 0} a_i X^i\right)\left(\sum_{j\geq 0} b_j X^j\right) = \sum_{i\geq 0}\left(\sum_{j+k=i,\ j\geq 0,\ k\geq 0} a_j b_k\right) X^i,$$

where all but finitely many coefficients are equal to zero. Define

$$R[X_1, \ldots, X_n] = R[X_1] \ldots [X_n] = \{\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} | a_{i_1,\ldots,i_n} \in R\},$$

where all but finitely many coefficients are equal to zero.

$\lhd$ Let k be an infinite field, and $f \in k[X_1, \ldots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in k^n$. (What about if k is a finite field? Consider $X^2 - X$ in $\mathbb{F}_2[X]$.)

The **ring of formal power series** with coefficients in R is the set

$$R[[T]] = \{a_0 + a_1 T + \ldots | a_i \in R\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i\geq 0} a_i T^i\right)\left(\sum_{j\geq 0} b_j T^j\right) = \sum_{i\geq 0}\left(\sum_{j+k=i,\ j\geq 0,\ k\geq 0} a_j b_k\right) T^i.$$

Define

$$R[[T_1, \ldots, T_n]] = R[[T_1]] \ldots [[T_n]].$$

$k[X_1, \ldots X_n]$ is an integral domain, and a UFD. $k[X_1]$ is in fact a PID but $k[X_1, \ldots X_n]$ is not a PID for $n > 1$. For example, the ideal (X_1, X_2) is not principal.

A monomial ideal in $k[X, Y]$ is given by $I = (X^{i_1} Y^{j_1}, X^{i_2} Y^{j_2}, \ldots, X^{i_t} Y^{j_t})$ for $i_s, j_s \in \mathbb{N}$. We can draw a picture of $k[X, Y]$ by drawing a k-basis for it, and specify a monomial ideal by drawing a staircase (in red) as follows:

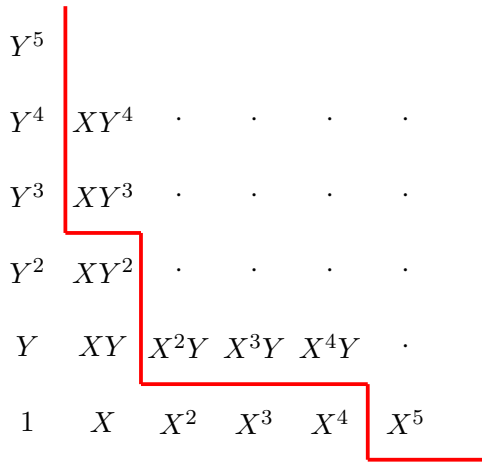


Figure 2: The monomial ideal $(XY^3, X^2Y, X^5) \subset k[X, Y]$.

A generating set of elements for a monomial ideal is given by the "corners" of the staircase.

The arithmetic cousin of $k[X, Y]$ is the ring $\mathbb{Z}[X]$.

$\lhd$ Let $\mathfrak{p} \subset \mathbb{Z}[X]$ be a prime ideal. Suppose $\mathfrak{p} \neq \mathbb{Z}[X]$ or (0). Show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Thus, $\mathfrak{p} \cap \mathbb{Z} = (p)$ where $p = 0$ or p is a prime number.

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = \{0\}$, then $\mathfrak{p} = (f)$ where $f \in \mathbb{Z}[X]$ is an irreducible polynomial.

(ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Then, $\mathfrak{p} = (p, f)$ where $f = 0$ or $f \in \mathbb{Z}[X]$ is a monic polynomial (leading coefficient is one) and its mod p reduction $\overline{f} \in \mathbb{F}_p[X]$ is irreducible.

In other words, to give a maximal ideal of $\mathbb{Z}[X]$ we have to choose a prime number $p \in \mathbb{Z}$ and an irreducible polynomial $\overline{f} \in \mathbb{F}_p[X]$ and then consider the ideal (p, f) where $f \in \mathbb{Z}[X]$ is any lift of $\overline{f}$ to a polynomial in $\mathbb{Z}[X]$. (Check that $(p, f) = (p, g)$ if $\overline{f} = \overline{g} \in \mathbb{F}_p[X]$).

The same argument will apply to any ring of the form $A[X]$ with A a PID.

$\lhd$ Formulate and prove the analogous result for $k[X, Y]$.

We next give two important examples of local rings; a geometric and an arithmetic example.

The power series ring $k[[X]]$ is a local ring with the unique maximal ideal $\mathfrak{m} = (X)$. To see this observe, that units in the power series ring are precisely the elements $f(X) = a_0 + a_1X + \ldots$ with $a_0 \neq 0$.

Let $p \in \mathbb{Z}$ be a prime number, the ring $\mathbb{Z}_{(p)} \coloneqq \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\} \subset \mathbb{Q}$ is a local ring with maximal ideal $\{\frac{a}{b} \in \mathbb{Z}_{(p)} : p \mid a\}$. Again, it is clear that the elements in this maximal ideal are precisely the non-units of $\mathbb{Z}_{(p)}$.

4 The ring $k[X_1, X_2, \ldots, X_n]$

4.1 Hilbert basis theorem

Theorem 4.1. *$k[X_1, X_2, \ldots, X_n]$ is Noetherian. More generally, if R is Noetherian, then $R[X]$ is also Noetherian.*

▶ We defined a Noetherian ring R to be ring such that all of its ideals are finitely generated. This turns out to be imply the condition that all ascending chains of ideals

$$I_1 \subset I_2 \subset I_3 \ldots$$

are eventually constant, that is, there exist a sufficiently large s such that $I_s = I_{s+i}$ for all $i \geq 0$. This condition is known as **Ascending Chain Condition (ACC)**.

Indeed, let $I = \bigcup_{i=1}^{\infty} I_i$. One can check directly that I is an ideal. Now, since it is finitely generated, we can write $I = (f_1, f_2, \ldots, f_m)$ for some elements $f_i \in R$. Each of the generators f_i is contained in some I_{j_i} so let s be the maximum of the j_i. Then, we have

$$I = (f_1, \ldots, f_m) \subset I_s \subset I_{s+1} \subset \ldots \subset I.$$

Hence the chain stabilises at I_s.

Conversely, suppose that every ascending chain stabilises and $I \subset R$ be an ideal. Let $f_1 \in I$. If $(f_1) = I$, we are done. Otherwise, let $f_2 \in I \setminus (f_1)$. If $(f_1, f_2) = I$, we are done. Otherwise, let $f_3 \in I \setminus (f_1, f_2)$. Continuing this way, we produce an ascending chain

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \ldots$$

which must stabilise at some point hence $I = (f_1, f_2, \ldots, f_m)$ for some m.

ƨ This argument is sometimes referred as Noetherian induction. When we make infinitely many choices f_i we use Axiom of Dependent choice; a countable version of Axiom of Choice. In the proof of Hilbert basis theorem given below, we only use the implication that Noetherian implies ACC. So, our proof does not depend on the Axiom of Choice.

Proof. (of Theorem 4.1) Let $I \subset R[X]$ be a nonzero ideal. We want to prove that I is finitely generated. Define the auxiliary ideals

$$J_n = \{a \in R : \exists f \in I \text{ such that } f = aX^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0\} \cup \{0\}$$

of leading coefficients of elements in I of degree n. It is easy to see that J_n is an ideal using the fact that I is an ideal. Moreover, $J_n \subset J_{n+1}$ since if $f \in I$, then $Xf \in I$. Therefore, we have an ascending chain of ideals

$$J_0 \subset J_1 \subset \ldots$$

Since R is Noetherian, this chain stabilises. So, we have $J_s = J_{s+i}$ for some s and for all $i \geq 0$.

Now, since R is Noetherian, for each $m \leq s$, we have that J_m is finitely generated. Thus, we can write $J_m = (a_{m,1}, a_{m,2}, \ldots, a_{m,r_m})$. By definition of J_m for each $a_{m,j}$ with $1 \leq j \leq r_m$, there is a polynomial $f_{m,j}$ of degree m with leading coefficient $a_{m,j}$.

Finally, we claim that $\{f_{m,j}\}_{0\leq m\leq s, 1\leq j\leq r_m}$ generate I. Indeed, for any $f \in I$, if f has degree m then its leading coefficient $a \in J_m$. Thus, if $m \geq s$, then $a \in J_m = J_s$ so that $a = \sum b_i a_{s,i}$ with $b_i \in R$. We can consider $f - \sum b_i X^{m-s} f_{s,i}$ which has degree less than m. Similarly, if $m \leq s$, then $a \in J_m$ so that $a = \sum b_i a_{m,i}$ with $b_i \in R$ and $f - \sum b_i f_{m,i}$ has degree less than m. By induction on m, it follows that f can be written as a linear combination of $\{f_{m,j}\}_{0\leq m\leq s, 1\leq j\leq r_m}$. □

▶ Not every subring of a Noetherian ring is Noetherian.

◁ Show that

$$R = \{f(X,Y) = \sum a_{ij} X^i Y^j | i, j \geq 0, \text{ and } i > 0 \text{ if } j \neq 0\}$$

is a subring of the Noetherian ring $k[X,Y]$ but R is not Noetherian.

◁ Prove that if R is Noetherian, $R[[T]]$ is also Noetherian.

Corollary 4.2. *Any finitely generated algebra over $\mathbb{Z}$ or over a field k is Noetherian.*

Proof. The assumption is that the ring is $R[X_1, \ldots, X_n]/I$ for some n and $R = \mathbb{Z}$ or $R = k$. We know that the ideals of $R[X_1, \ldots, X_n]/I$ are images of the ideals of $R[X_1, \ldots, X_n]$ that contain I. The latter are finitely generated by the fact that $A[X_1, \ldots, X_n]$ is Noetherian. □

4.2 Affine varieties

Let $S \subset k[X_1, \ldots, X_n]$. We let the **affine variety** defined by S to be

$$\mathcal{V}(S) = \{(x_1, \ldots, x_n) \in k^n : f(x_1, \ldots, x_n) = 0 \text{ for all } f \in S\}$$

Note that if we set $I = (S)$ the ideal generated by S and apply Hilbert basis theorem to write $I = (f_1, \ldots, f_h)$ for some finite number of polynomials, then

$$\mathcal{V}(S) = \mathcal{V}(I) = \mathcal{V}(\{f_1, \ldots, f_h\})$$

hence every affine variety is defined as the vanishing locus of a finite set of polynomials.

Given a subset $U \subset k^n$, we define an ideal

$$\mathcal{I}(U) = \{f \in k[X_1, \ldots, X_n] : f(x_1, x_2, \ldots, x_n) = 0 \text{ for all } (x_1, x_2, \ldots, x_n) \in U\}$$

Thus, we have maps between subsets of k^n and subsets of $k[X_1, \ldots, X_n]$.

$$\{S \subset k[X_1, \ldots, X_n]\} \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \{U \subset k^n\}$$

◁ Note that $U \subset \mathcal{V}(\mathcal{I}(U))$ for any subset $U \subset k^n$. Prove that if U is an affine variety, then $U = \mathcal{V}(\mathcal{I}(U))$.

In general, for a set $U \subset k^n$, $\mathcal{V}(\mathcal{I}(U))$ is the smallest affine variety containing U, and is called the **Zariski closure** of U and denoted by $\overline{U}$.

▶ $\mathcal{V}(I+J) = \mathcal{V}(I) \cap \mathcal{V}(J)$.

▶ $\mathcal{V}(IJ) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

▶ Hilbert's Nullstellensatz which we will see later in the course implies that if k is algebraically closed, $\mathcal{V}(I : J^\infty) = \overline{\mathcal{V}(I) \setminus \mathcal{V}(J)}$.

Basic questions:

- Let $f_1, f_2, \ldots, f_n \in k[X_1, \ldots, X_n]$ and $I = (f_1, f_2, \ldots, f_n)$. Given $f \in k[X_1, \ldots, X_n]$, how can we decide if $f \in I$? Does f vanish on the affine variety $U = \mathcal{V}(I)$ defined by I?
- Suppose $U = \mathcal{V}(S) \subset k^n$ is non-empty, what is the dimension of U ?
- $S \subset k[X_1, \ldots, X_n]$, is it true that $\mathcal{V}(S) \neq \emptyset$?

We will answer all these question in the next few sections but first we have to develop some tools.

4.3 Gröbner basis

We work in the ring $k[X_1, \ldots, X_n]$. Let us introduce some notation.

$\mathbb{N}^n = \{\alpha = (\alpha_1, \ldots, \alpha_n) : \alpha_i \in \mathbb{N}\}$.

$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$. We write $|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$ for the total degree of X^α.

We write an element $f \in k[X_1, \ldots, X_n]$ as $f = \sum_\alpha a_\alpha X^\alpha$ with $a_\alpha \in k$ such that $\{\alpha : a_\alpha \neq 0\}$ is a finite set.

Unlike the case of $k[X]$ when $n > 1$, it is unclear what monomial is the highest degree. For example, what is the highest degree monomial in $f(X, Y) = X^2Y + 42XY^2$?

To address this we introduce the following notion.

Definition 4.3. *Let $\leq$ be a total ordering on $\mathbb{N}^n$. We say that $\leq$ is a* **monomial ordering** *if*

- $0 = (0, \ldots, 0) \leq \alpha$ *for all* $\alpha \in \mathbb{N}^n$.
- *If* $\alpha \leq \beta$, *then* $\alpha + \gamma \leq \beta + \gamma$ *for all* $\gamma \in \mathbb{N}^n$.

◁ Show that $X^\alpha | X^\beta$ implies that $\alpha \leq \beta$ for any monomial ordering $\leq$.

▶ Lexicographic Order $\leq_{lex}$: Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$. Define $\alpha \leq \beta$ if there exists an $i \in \{1, \ldots, n\}$ such that $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_{i-1} = \beta_{i-1}$ and $\alpha_i < \beta_i$.

▶ Graded Lexicographic Order $\leq_{grlex}$: Define $\alpha \leq \beta$ if either $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and $\alpha \leq_{lex} \beta$.

◁ Order the terms of the polynomial $f(X, Y, Z) = XY^2Z + Z^2 + X^3 + X^2Z^2$ with respect to $\leq_{lex}$ and $\leq_{grlex}$.

▶ Given a matrix $A \in GL(n, \mathbb{R})$ we can define a monomial ordering on $k[X_1, \ldots, X_n]$ by setting $\beta \leq_A \alpha$ if and only if $A\beta \leq_{lex} A\alpha$. In fact, any monomial ordering on $k[X_1, X_2, \ldots, X_n]$ can be defined this way for some matrix A.[3]

■ In what follows, we fix a monomial ordering $\leq$.

■ For $\alpha, \beta \in \mathbb{N}^n$, we often write $X^\alpha \leq X^\beta$ to mean that $\alpha \leq \beta$.

Given a polynomial

$$f = a_{\alpha^{(1)}} X^{\alpha^{(1)}} + a_{\alpha^{(2)}} X^{\alpha^{(2)}} + \ldots + a_{\alpha^{(s)}} X^{\alpha^{(s)}}$$

where $\alpha^{(i)} \in \mathbb{N}^n$ with $\alpha^{(1)} > \alpha^{(2)} > \ldots > \alpha^{(s)}$, we define

$$\begin{aligned} LT(f) &\coloneqq a_{\alpha^{(1)}} X^{\alpha^{(1)}} && \textbf{leading term} \\ LM(f) &\coloneqq X^{\alpha^{(1)}} && \textbf{leading monomial} \\ LC(f) &\coloneqq a_{\alpha^{(1)}} && \textbf{leading coefficient} \end{aligned}$$

The ideal membership problem is easy to solve for monomial ideals.

Lemma 4.4. *Let $I \subset k[X_1, \ldots, X_n]$ be a monomial ideal generated by a set G of monomials and $f \in k[X_1, \ldots, X_n]$ then $f \in I$ if and only if every term of f is divisible by a monomial in G.*

Proof. Suppose $f \in I$, then $f = \sum_{i=1}^{s} h_i g_i$ for some polynomials $h_i \in k[X_1, \ldots, X_n]$ and monomials $g_i \in G$. Write $h_i = \sum a_{i,\alpha} X^\alpha$, then $f = \sum_{i,\alpha} a_{i,\alpha} X^\alpha g_i$. Hence, all the terms of f are divisible by monomials in G. The other direction is clear. □

Lemma 4.5. *Let $(g_i)_{i \geq 1}$ be a sequence of monomials such that $g_1 \geq g_2 \geq g_3 \geq \ldots$. Then, there exists $r \geq 1$ such that $g_r = g_{r+1} = g_{r+2} = \ldots$.*

Proof. Let $I = (g_i : i \geq 1)$. By Hilbert's basis theorem, there exists r such that $I = (g_1, \ldots, g_r)$. Now, for $i > r$, we have $g_i \leq g_r$. On the other hand, since $g_i \in I$, by the previous lemma, there exists $j \in \{1, \ldots, r\}$ such that $g_j | g_i$. Hence, $g_r \leq g_j \leq g_i$ hence $g_i = g_r$. □

Proposition 4.6. (Division with remainder) *Let $f, f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ non-zero polynomials. Then, there exist polynomials $h_1, \ldots, h_s, r$ such that*

$$f = h_1 f_1 + h_2 f_2 + \ldots + h_s f_s + r$$

with the following properties

- *$LT(h_i f_i) \leq LT(f)$ for all i with $h_i \neq 0$.*
- *$r = 0$ or none of the terms of r is divisible by $LT(f_i)$ for all i and $LT(r) \leq LT(f)$*

[3] L Robbiano - Term orderings on the polynomial ring.

Proof. Suppose that there exists an i such that $LT(f_i)|LT(f)$. Then let

$$\tilde{f} = f - \frac{LT(f)}{LT(f_i)} f_i$$

If $\tilde{f} = 0$, then we stop by setting $r = 0$. Otherwise, we have $LT(\tilde{f}) < LT(f)$. By induction, we can write

$$\tilde{f} = \tilde{h}_1 f_1 + \ldots \tilde{h}_s f_s + r$$

with the required conditions. Then we can write

$$f = h_1 f_1 + \ldots h_s f_s + r$$

where $h_j = \tilde{h}_j$ for $j \neq i$ and $h_i = \tilde{h}_i + \frac{LT(f)}{LT(f_i)}$. It is easy to check that the required conditions are satisfied.

If there does no exist i such that $LT(f_i)|LT(f)$. Then, we let $\tilde{f} = f - LT(f)$. Again, if $\tilde{f} = 0$, we stop by setting $h_i = 0$ and $r = f$. Otherwise, by induction, we can write $\tilde{f} = h_1 f_1 + \ldots h_s f_s + \tilde{r}$. Then, we set

$$f = h_1 f_1 + \ldots h_s f_s + r$$

where $r = \tilde{r} + LT(f)$. □

Example. Let $f = XY^2 - X, f_1 = XY + 1, f_2 = Y^2 - 1$. Leading terms are XY^2, XY, Y^2 respectively. Since $XY|XY^2$, we can write $\tilde{f} = f - Yf_1 = -X - Y$. Hence,

$$f = Yf_1 + 0f_2 + (-X - Y)$$

Another possibility is to use that $Y^2|XY^2$, then we have $\tilde{f} = f - Xf_2 = 0$, so we get

$$f = 0f_1 + Xf_2 + 0$$

Hence, the remainder r is not unique (depends on the ordering of $f_1, f_2, \ldots, f_s$).

We can implement the division with remainder algorithm in Macaulay 2 as follows.

```
div = (f,G) -> (
R := ring f; p := f; r := 0_R; s := #G; Q := new MutableHashTable;
for j from 0 to s-1 do Q#j = 0_R;
while p != 0 do (
     i := 0;
     while i < s and leadTerm(p) % leadTerm(G#i) != 0 do i = i+1;
        if i < s then (
           Q#i = Q#i + (leadTerm(p) // leadTerm(G#i));
           p = p - (leadTerm(p) // leadTerm(G#i)*G#i))
        else (
           r = r + leadTerm(p);
           p = p - leadTerm(p)));
L := apply(s, j -> Q#j);
return (r,L));
```

Using the above division function, you can do division in Macaulay 2 as follows.

```
R = QQ[X,Y]
f= X*Y^2 - X
f1 = X*Y +1
f2 = Y^2 - 1
G = {f1,f2}
div(f,G)
G = {f2,f1}
div(f,G)
```

Definition 4.7. *(Buchberger) Let I be a non-zero ideal. A subset $G \subset I \setminus \{0\}$ is called a Gröbner basis of I if $|G| < \infty$ and generates the* **initial ideal** *of I, that is*

$$\mathfrak{in}(I) \coloneqq (LT(f) : 0 \neq f \in I) = (LT(g) : g \in G)$$

► If $I = (f_1, f_2, \ldots, f_s)$ then it may not be the case that $\mathfrak{in}(I) = (LT(f_1), LT(f_2), \ldots, LT(f_s))$.

◁ Take $I = (f_1, f_2)$ with $f_1 = X^3 - 2XY$ and $f_2 = X^2Y - 2Y^2 + X$ and use $\leq_{grlex}$. Show that $(LT(f_1), LT(f_2))$ is strictly contained in $\mathfrak{in}(I)$.

If you want to check your calculations, you can ask Macaulay 2 for help as follows:

```
R = QQ[x,y, MonomialOrder=> GLex];
I = ideal (x^3-2*x*y, x^2*y-2*y^2+x);
inI = ideal leadTerm I
```

Note that the initial ideal depends on the monomial order you choose.

```
R = QQ[x,y, MonomialOrder=> Lex];
I = ideal (x^3-2*x*y, x^2*y-2*y^2+x);
inI = ideal leadTerm I
```

Theorem 4.8. *(Buchberger) Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $I \subset k[X_1, \ldots, X_n]$.*

1. *Given an element $f \in k[X_1, \ldots, X_n]$. Using division with remainder, we write*

$$f = h_1 g_1 + h_2 g_2 + \ldots + h_s g_s + r.$$

   Then, $r = 0$ if and only if $f \in I$ and $I = (G)$. Moreover, r is independent of the ordering of $g_1, g_2, \ldots, g_s$.

2. *Let $C(I) \coloneqq \{\alpha \in \mathbb{N}^n : LT(g_i) \nmid X^\alpha \text{ for all } g_i\}$. Then $\{X^\alpha + I : \alpha \in C(I)\}$ is a k-vector space basis of $k[X_1, \ldots, X_n]/I$.*

Proof. Suppose $f \in I$ and $r \neq 0$, then $r = f - \sum_{i=1}^{s} h_i g_i \in I$. Hence,

$$LT(r) \in (LT(g_1), LT(g_2), \ldots, LT(g_s)).$$

By Lemma 4.4, there exists i such that $LT(g_i)|LT(r)$. This contradicts with the properties of the division with remainder. Hence $r = 0$. (The other direction of the claim is obvious). It also follows that $I = (G)$.

Suppose $f = \sum_{i=1}^{s} h_i g_i + r = \sum_{i=1}^{s} k_i g_i + \tilde{r}$ after division with remainder. Then $\sum_{i=1}^{s}(h_i - k_i)g_i = \tilde{r} - r \in I$. If $\tilde{r} \neq r$, then $LT(\tilde{r} - r) \in \mathfrak{in}(I) = (LT(g) : g \in G)$. Hence, there exists i such that $LT(g_i)|LT(\tilde{r} - r)$. This is a contradiction with the conditions on r, $\tilde{r}$ imposed by the division with remainder. Hence $r = \tilde{r}$.

After division with remainder, we have that none of the terms of r is divisible by $LT(g_i)$. Thus, r is a k-linear combination of monomials X^α with $\alpha \in C(I)$. Hence, $k[X_1, \ldots, X_n]/I$ is generated by $\{X^\alpha + I : \alpha \in C(I)\}$.

Suppose that $\sum_{i=1}^{m} a_i X^{\alpha_i} \in I$ for $\alpha_i \in C(I)$. We divide it by $g_1, \ldots, g_s$, we get

$$\sum_{i=1}^{m} a_i X^{\alpha_i} = 0 \cdot g_1 + 0 \cdot g_2 + \ldots + 0 \cdot g_s + r \in I$$

since for all i we have $\alpha_i \in C(I)$. Moreover, $r = 0$ by the first part because $\sum_{i=1}^{m} a_i X^{\alpha_i} \in I$. Thus, $X^\alpha + I$ for $\alpha \in C(I)$ are linearly independent. □

Corollary 4.9. *The variety $\mathcal{V}(I) \subset k^n$ defined by I has finitely many points if $C(I)$ is finite.*

Proof. By the theorem $C(I)$ being finite means that the ring $k[X_1, \ldots, X_n]/I$ is finite-dimensional as a vector space. Now for a fixed i, consider the monomials $1, X_i, X_i^2, \ldots$. Since $k[X_1, \ldots, X_n]/I$ is finite-dimensional, it follows that there exist $c_0, c_1, c_2, \ldots, c_m \in k$ for some m such that

$$c_0 + c_1 X_i + c_2 X_i^2 + \ldots + c_m X_i^m \in I$$

hence, this polynomial vanishes on $\mathcal{V}(I)$ but a polynomial of one variable can have at most finitely many roots. It follows that the i-th co-ordinates of points in $\mathcal{V}(I)$ can only take finitely many values. Same is true for all i, hence $\mathcal{V}(I)$ is finite. □

Theorem 4.8 gives an algorithm for solving the ideal membership problem provided that we know a Gröbner basis for the ideal.

Problem: How to construct a Gröbner basis?

Definition 4.10. *Let $f, g \in k[X_1, \ldots, X_n]$ be nonzero polynomials. Let $X^\alpha = LM(f)$ with $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $X^\beta = LM(g)$ with $\beta = (\beta_1, \ldots, \beta_n)$. Define $\gamma = (\gamma_1, \ldots, \gamma_n)$ with $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all i, i.e. $X^\gamma = \operatorname{lcm}(LM(f), LM(g))$. The S-polynomial of f and g is defined to be*

$$S(f, g) = \frac{X^\gamma}{LT(f)} f - \frac{X^\gamma}{LT(g)} g$$

Example. Let $f = 4X^2Z - 7Y^2$ and $g = XYZ^2 + 3XZ^4$ using the $\leq_{lex}$ order, we see that $\operatorname{lcm}(LM(f), LM(g)) = X^2YZ^2$, and

$$S(f,g) = \frac{X^2YZ^2}{4X^2Z}f - \frac{X^2YZ^2}{XYZ^2}g = (1/4)YZf - Xg = -3X^2Z^4 - (7/4)Y^3Z$$

Here is how you may do this in Macaulay 2:

```
R = QQ[x,y,z, MonomialOrder => Lex];
f = 4*x^2*z-7*y^2;
g = x*y*z^2 + 3*x*z^4;
Spoly = (f,g) -> lcm(leadMonomial(f), leadMonomial(g))/ leadTerm(f)*f
      - lcm(leadMonomial(f),leadMonomial(g))/leadTerm(g)*g;
Spoly(f,g)
```

▶ $LM(S(f,g)) < \operatorname{lcm}(LM(f), LM(g))$. In this sense, we can say that the S-polynomial is designed to produce cancellation of leading terms.

The name S-polynomial is short for "syzygy polynomial". You can blame Cayley if you don't know how to pronounce the word syzygy. In general, syzygy is a kind of linear relation. Here it is a linear relation between polynomials in several variables with polynomial coefficients. In astronomy, it means a linear relation between positions of planets.

Theorem 4.11. *(Buchberger's criterion) Let $I \subset k[X_1, \ldots, X_n]$ be a non-zero ideal. $G = \{g_1, \ldots, g_s\} \in I \setminus \{0\}$ such that $I = (g_1, \ldots, g_s)$. Then, G is a Gröbner basis for I if and only if for all $1 \leq i < j \leq s$, the remainder of the division with remainder of $S(g_i, g_j)$ by $\{g_1, \ldots, g_s\}$ is 0.*

For the proof of this theorem, we will need the following technical result. The idea is that every cancellation of leading terms among polynomials of the same leading monomial comes from the cancellation that occurs for S-polynomials.

Lemma 4.12. *Suppose $g_1, \ldots, g_s \in k[X_1, \ldots, X_n]$, $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^n$ and $c_1, \ldots, c_s \in k \setminus \{0\}$. Let*

$$f \coloneqq \sum_{i=1}^{s} c_i X^{\alpha_i} g_i \in k[X_1, \ldots, X_n]$$

Suppose that for all i, $LM(X^{\alpha_i} g_i) = X^{\alpha_i} LM(g_i) = X^\delta$ for some $\delta \in \mathbb{N}^n$ and $LM(f) < X^\delta$. Then, we have

$$f = \sum_{1 \leq i < j \leq s} c_{ij} X^{\delta - \gamma_{ij}} S(g_i, g_j)$$

for some $c_{ij} \in k$ and $\gamma_{ij} = \operatorname{lcm}(LM(g_i), LM(g_j))$. Moreover, $LM(X^{\delta - \gamma_{ij}} S(g_i, g_j)) < X^\delta$.

Proof. Multiplying the c_i by the leading coefficient of g_i, we can suppose that $LC(g_i) = 1$ for all i. Thus, without loss of generality, we assume $LT(g_i) = LM(g_i)$.

We define

$$\begin{aligned} g &\coloneqq f - c_1 X^{\delta-\gamma_{12}} S(g_1, g_2) \\ &= c_1 X^{\alpha_1} g_1 + c_2 X^{\alpha_2} g_2 + \sum_{i=3}^{s} c_i X^{\alpha_i} g_i - c_1 X^{\delta-\gamma_{12}} \left(\frac{X^{\gamma_{12}}}{LM(g_1)} g_1 - \frac{X^{\gamma_{12}}}{LM(g_2)} g_2 \right) \\ &= c_1 \left(X^{\alpha_1} - \frac{X^{\delta}}{LM(g_1)} \right) g_1 + \left(c_2 X^{\alpha_2} + c_1 \frac{X^{\delta}}{LM(g_2)} \right) g_2 + \sum_{i=3}^{s} c_i X^{\alpha_i} g_i \\ &= (c_1 + c_2) X^{\alpha_2} g_2 + \sum_{i=3}^{s} c_i X^{\alpha_i} g_i \end{aligned}$$

where the coefficient of g_1 vanishes because $X^{\alpha_1} LM(g_1) = X^{\delta}$ by assumption. Now, g satisfies all the hypothesis but we have decreased the number of terms. Thus the proof of the first assertion follows by induction on s. (Note that in the case $s = 2$, by assumption we must have $c_1 + c_2 = 0$ so as to have $LM(f) < X^{\delta}$ hence we must have $f = c_1 X^{\delta-\gamma_{12}} S(g_1, g_2)$.)

We have $X^{\delta} = X^{\alpha_i} LM(g_i) = X^{\alpha_j} LM(g_j)$ for all $1 \leq i < j \leq s$. Hence, $LM(g_i)$ and $LM(g_j)$ both divide X^{δ}. Thus, $X^{\gamma_{ij}} | X^{\delta}$.

$$S(g_i, g_j) = \frac{X^{\gamma_{ij}}}{LM(g_i)} g_i - \frac{X^{\gamma_{ij}}}{LM(g_j)} g_j$$

Since, the leading terms cancel, we have $LM(S(g_i, g_j)) < X^{\gamma_{ij}}$. □

We are now ready to give the proof of the theorem.

Proof. (of Theorem 4.11) One direction is easy: Suppose G is Gröbner basis, then since $S(g_i, g_j) \in I$ division with remainder by G will give the zero remainder. Conversely, suppose $f \in I$, we have to show that $LT(f) \in (LT(g_1), \ldots, LT(g_s))$. Write

$$f = \sum_{i=1}^{s} u_i g_i \text{ with } u_i \in k[X_1, \ldots, X_n]$$

Let $X^{\delta} = \max\{LM(u_i g_i) : 1 \leq i \leq s, u_i \neq 0\}$. We have $LM(f) \leq X^{\delta}$.

Case 1: Suppose $LM(f) = X^{\delta}$, then

$$LT(f) = \sum_{\substack{1 \leq i \leq s, \\ LT(u_i g_i) = X^{\delta}}} LT(u_i g_i) = \sum_{\substack{1 \leq i \leq s, \\ LT(u_i g_i) = X^{\delta}}} LT(u_i) LT(g_i) \in (LT(g_1), \ldots, LT(g_s)).$$

Case 2: If $LM(f) < X^{\delta}$, we define

$$f^* = \sum_{\substack{1 \leq i \leq s, \\ LM(u_i g_i) = X^{\delta}}} LT(u_i) g_i$$

Since $LM(f^*) < X^\delta$, applying the Lemma 4.12, we may write

$$f^* = \sum_{1 \leq i < j \leq s} c_{ij} X^{\alpha_{ij}} S(g_i, g_j) \quad \text{with} \quad X^{\alpha_{ij}} LM(S(g_i, g_j)) < X^\delta.$$

Now, by assumption, division by remainder gives

$$S(g_i, g_j) = \sum_{k=1}^{s} v_k g_k \text{ with } v_k \in k[X_1, \ldots, X_n] \quad \text{and} \quad LM(v_k g_k) \leq LM(S(g_i, g_j))$$

Therefore, $X^{\alpha_{ij}} S(g_i, g_j) = \sum_{k=1}^{s} (X^{\alpha_{ij}} v_k) g_k$ and $LM(X^{\alpha_{ij}} v_k g_k) < X^\delta$. It follows that there exist polynomials $u_i^* \in k[X_1, \ldots, X_n]$ such that

$$f^* = \sum_{i=1}^{s} u_i^* g_i \quad \text{with} \quad LM(u_i^* g_i) < X^\delta$$

By construction, we also have polynomials $v_i^* \in k[X_1, \ldots, X_n]$ such tat

$$f - f^* = \sum_{i=1}^{s} v_i^* g_i \quad \text{with} \quad LM(v_i^* g_i) < X^\delta$$

Hence, we can write

$$f = (f - f^*) + f^* = \sum_{i=1}^{s} (u_i^* + v_i^*) g_i \quad \text{with} \quad LM((u_i^* + v_i^*) g_i) < X^\delta$$

With this new expression of f, we go back to the beginning of the proof. If we are in the first case, we are done. Otherwise, repeat the procedure in the second case to decrease δ. This procedure has to stop after finitely many steps. □

Finally, let us explain how the results we have covered so far provides an algorithm for constructing a Gröbner basis (hence, an algorithm for determining whether a polynomial belongs to an ideal I).

Suppose, we are given $f_1, \ldots, f_t \in k[X_1, \ldots, X_n]$ such that $I := (f_1, \ldots, f_t)$ and we fix a monomial order $\leq$.

Initialize with $G = \{f_1, \ldots, f_t\}$. Now, suppose $G = \{g_1, \ldots, g_s\}$. For $1 \leq i < j \leq s$ divide $S(g_i, g_j)$ with remainder by G. Let r_{ij} denote the remainder. If $r_{ij} = 0$ for all i, j, then stop. Then G is a Gröbner basis. If there exist i, j such that $r_{ij} \neq 0$. Then, change G with $G \cup \{r_{ij}\}$ and continue.

Proposition 4.13. *The procedure described above stops in finitely many steps.*

Proof. By applying the procedure, we obtain a chain of sets

$$G_0 = \{f_1, \ldots, f_t\} \subset G_1 \subset G_2 \subset \ldots$$

We have

$$(LT(G_0)) \subset (LT(G_1)) \subset (LT(G_2)) \subset \dots$$

is an ascending chain of ideals in $k[X_1, \dots, X_n]$. Since $k[X_1, \dots, X_n]$ is Noetherian (by Hilbert), there exists m such that $(LT(G_m)) = (LT(G_{m+1})) = (LT(G_{m+2})) = \dots$. The procedure stops with $G_m = \{g_1, \dots, g_s\}$. Suppose $h, g \in G_m$. Division with remainder gives $S(g,h) = \sum_{i=1}^{s} h_i g_i + r$. Suppose that $r \neq 0$, $LT(r) \in (LT(G_m))$. Hence, there exists i, such that $LT(g_i) | LT(r)$. This contradicts to the conditions on r. Hence, $r = 0$. □

▶ Note that the algorithmic construction of Gröbner basis gives another (constructive) approach to proving Hilbert's basis theorem for a general ideal I. By elementary techniques, one first proves Dickson's lemma, i.e. any monomial ideal is finitely generated, and then uses the above argument to deduce the existence of a (finite) Gröbner basis for any ideal.

◁ Compute a Gröbner basis (by hand) for the ideal $I = (X^2, XY + Y^2)$.

▶ Here is an example of how you can compute Gröbner basis in Macaulay 2:

```
R = QQ[x,y,z, MonomialOrder => Lex]
I = ideal (x^2-z-1,z^2-y-1,x*y^2-x-1)
gens gb I
```

◁ (Elimination theory) Let $I \subset k[X_1, \dots, X_n]$ be a non-zero ideal, G a Gröbner basis for I with respect to the $\leq_{lex}$ order. Then $G \cap k[X_{l+1}, \dots, X_n]$ generates the ideal $I \cap k[X_{l+1}, \dots, X_n]$ for all $0 \leq l \leq n$.

A Gröbner basis $G = \{g_1, \dots, g_s\}$ of an ideal I is said to be **reduced** if $LC(g_i) = 1$ for all i and for all i none of the terms of g_i is divisible by any of the $LT(g_j)$ for $j \neq i$. Starting from any Gröbner basis G, it is easy to produce a reduced Gröbner basis First, if for $g \in G$, we have $LT(g) \in (LT(g_i) : g_i \in G, g_i \neq g)$, then replace G with $G \setminus \{g\}$. Next, if any g_i has a term divisible by $LT(g_j)$ for some j, replace g_i by the remainder of the division of g_i by g_j. Finally, make sure that $LC(g_i) = 1$ for all i by rescaling with an element of k. It is easy to see that this gives a reduced Gröbner basis. An important property is that an ideal I has a unique reduced Gröbner basis with respect to a fixed monomial order. This is an easy result to prove but we omit the proof in order to save time for other topics.

▶ Consider the ideal $I = (X - Z^2, Y - Z^3)$ in $k[X, Y, Z]$. For the lexicographic order with $X > Y > Z$, it is easy to verify that $(X - Z^2, Y - Z^3)$ is the reduced Gröbner basis. On the other hand, for the graded lexicographic order with $X > Y > Z$, it is easy to verify that $(X^2 - YZ, XZ - Y, Z^2 - X)$ is the reduced Gröbner basis. This example shows that the number of elements in the reduced Gröbner basis for a given ideal depends on the monomial ordering.

4.4 Hilbert polynomial

Problem: How to measure the "size" of an ideal I, or equivalently "dimension" of the affine variety $\mathcal{V}(I)$?

Definition 4.14. *Let $I \subset k[X_1, \ldots, X_n]$ be an ideal and $s \in \mathbb{N}$, and let us write*

$$k[X_1, \ldots, X_n]_{\leq s} \coloneqq \{f \in k[X_1, \ldots, X_n] : f = 0 \text{ or } \deg(f) \leq s\}$$

and

$$I_{\leq s} \coloneqq I \cap k[X_1, \ldots, X_n]_{\leq s}$$

We define

$$HF_I(s) = \dim_k \left(\frac{k[X_1, \ldots, X_n]_{\leq s}}{I_{\leq s}} \right) < \infty$$

Hilbert function of I, as a function $HF_I : \mathbb{N} \to \mathbb{N}$.

Example. (a) Let $I = k[X_1, \ldots, X_n]$. Then $HF_I(s) = 0$ for all $s \in \mathbb{N}$.

(b) Let $I = \{0\}$ Then

$$\begin{aligned} HF_I(s) &= \dim_k k[X_1, \ldots, X_n]_{\leq s} \\ &= \text{ number of monomials } X^\alpha \text{ with } |\alpha| \leq s \\ &= \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \alpha_1 + \ldots + \alpha_n \leq s\} = \binom{s+n}{n} \\ &= \frac{1}{n!}(s+n)(s+n-1)\cdots(s+1) = \frac{1}{n!}s^n + \frac{1}{n!}\binom{n+1}{2}s^{n-1} + \ldots + \sum_{i=1}^{n} \frac{1}{i}s + 1 \end{aligned}$$

is a polynomial of degree n.

(c) Suppose that $I = (f)$ where $f \in k[X_1, \ldots, X_n]$ with $deg(f) = d \geq 0$. Then

$$HF_I(s) = \dim_k k[X_1, \ldots, X_n]_{\leq s} - \dim_k I_{\leq s}$$

We have

$$I_{\leq s} = \{g \cdot f | g \in k[X_1, \ldots, X_n], deg(g) + d \leq s\}$$

Thus, if $s < d$, then $I_{\leq s} = \{0\}$. If $s \geq d$, then $\dim_k I_{\leq s} = |\{X^\alpha : |\alpha| \leq s - d\}|$. Hence,

$$\begin{aligned} HF_I(s) &= \binom{n+s}{n} \text{ if } \quad s < d \\ &= \binom{n+s}{n} - \binom{n+s-d}{n} = \frac{d}{(n-1)!}s^{n-1} + \text{lower order terms. if } \quad s \geq d \end{aligned}$$

Lemma 4.15. *(Macaulay) Let us equip $k[X_1, \ldots, X_n]$ with graded lexicographic order $\leq_{grlex}$. Let I be an ideal, and $\mathfrak{in}(I) = (LT(f) : f \in I)$. Then,*

$$HF_I(s) = HF_{\mathfrak{in}(I)}(s) \quad \textit{for all} \quad s \geq 0.$$

Proof. $I_{\leq s}$ contains only a finite number of monomials

$$\{LM(f) : f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}$$

where $f_1, \ldots, f_m \in I_{\leq s}$ and $LM(f_1) > LM(f_2) > \ldots > LM(f_m)$.

We will show that (a) $\{f_1, \ldots, f_m\}$ is a k-basis of $I_{\leq s}$, (b) $\{LM(f_1), \ldots, LM(f_m)\}$ gives a k-basis for $\mathfrak{in}(I)_{\leq s}$. (This implies the stated result.)

Linear independence for (a): Suppose there exists a_i not all zero such that $\sum_{i=1}^{m} a_i f_i = 0$. Choose the smallest $i = i_0$ such that $a_{i_0} \neq 0$. Then

$$0 = a_{i_0} f_{i_0} + a_{i_0+1} f_{i_0+1} + \ldots + a_m f_m$$

but $LM(f_i) < LM(f_{i_0})$, so we have a contradiction.

Linear independence for (b): clear.

Generation for (a): Let $f \in I_{\leq s}$. Then $LM(f) = LM(f_i)$ for some i. Hence $LT(f) = cLT(f_i)$ for some $c \in k$. Consider $f' = f - cf_i \in I_{\leq s}$. If $f' = 0$, then $f = cf_i$ as desired. Otherwise, $LM(f') < LM(f)$ (strictly smaller). Hence, repeat the argument with f'.

Generation for (b): Let $g \in \mathfrak{in}(I)_{\leq s}$. Then $g = \sum_j h_j LT(g_j)$ for some $h_j \in k[X_1, \ldots, X_n]$ and $g_j \in I$. We write $h_j = \sum_\alpha a_{\alpha,j} X^{\alpha_j}$ with $a_{\alpha,j} \in k$. Hence, $g = \sum_{j,\alpha} a_{\alpha,j} X^{\alpha_j} LT(g_j) = \sum_{j,\alpha} a_{\alpha,j} LT(X^{\alpha_j} g_j)$. Since $X^{\alpha_j} g_j \in I$, by letting $g_{\alpha,j} = X^{\alpha_j} g_j$, we can write $g = \sum_{\alpha,j} a_{\alpha,j} LT(g_{\alpha,j})$ with $a_{\alpha,j} \in k$ and $g_{\alpha,j} \in I$. Now, $LT(g_{\alpha,j}) \leq LT(g)$, hence (using the graded lex order) we see that $deg(g_{\alpha,j}) \leq deg(g) \leq s$. Therefore, g is a linear combination of $LM(f_1), \ldots, LM(f_m)$. $\square$

Theorem 4.16. *Let $I \subset k[X_1, \ldots, X_n]$. There exists a unique polynomial, called the Hilbert polynomial, $HP_I(t) \in \mathbb{Q}[t]$ and a positive number $s_0 \geq 0$ such that*

$$HF_I(s) = HP_I(s) \quad \textit{for all} \quad s \geq s_0$$

If $I = k[X_1, \ldots, X_n]$ then $HP_I(t) = 0$, otherwise $HP_I(t) \neq 0$. Write

$$HP_I(t) = a_d t^d + a_{d-1} t^{d-1} + \ldots + a_0$$

then $a_i d! \in \mathbb{Z}$ for all i and $a_d d! > 0$.

Proof. By the previous lemma, we may assume without loss of generality that $I = \mathfrak{in}(I) = (X^{\beta^{(1)}}, \ldots, X^{\beta^{(m)}})$ is a monomial ideal with $\beta^{(i)} \in \mathbb{N}^n$. Now, since I is a monomial ideal, a polynomial f is in I if and only if each term of f is divisible by an $X^{\beta^{(i)}}$ for some i. Therefore $f \in I_{\leq s}$ is generated by $\{X^\alpha : |\alpha| \leq s \text{ and } X^{\beta^{(i)}} \mid X^\alpha \text{ for some } i\}$. Put $C(I) \coloneqq \{\alpha \in \mathbb{N}^n : X^{\beta^{(i)}} \nmid X^\alpha \text{ for any } i\}$ and $C(I)_{\leq s} \coloneqq \{\alpha \in \mathbb{N}^n : |\alpha| \leq s, \alpha \in C(I)\}$. Thus, it follows that

$$HF_I(s) = |C(I)_{\leq s}|.$$

Next, we need to compute $|C(I)_{\leq s}|$. We will show that $C(I)$ is a finite union of translates of coordinate subspaces, which we denote as follows: for $J \subset \{1, 2, \ldots, n\}$ and a function $\tau : J \to \mathbb{N}$, we set

$$C(J, \tau) \coloneqq \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \alpha_j = \tau(j) \text{ for all } j \in J\}$$

Extend τ to $\{1, \ldots, n\}$ by setting $\tau(i) = 0$ for $i \notin J$. Then

$$C(J, \tau) = \{(\alpha_1 + \tau(1), \ldots, \alpha_n + \tau(n)) : \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n \text{ such that } \alpha_j = 0 \text{ for all } j \in J\}$$

Let $\tau = \sum_{j \in J} \tau(j)$. We have

$$|C(J, \tau)_{\leq s}| = |\{\alpha \in \mathbb{N}^n : |\alpha| \leq s - |\tau| \text{ and } \alpha_j = 0 \text{ for all } j \in J\}| = \binom{n - |J| + s - |\tau|}{n - |J|}$$
$$= \frac{1}{d!}(s^d + \text{ lower order terms })$$

provided $s > |\tau|$, in which case it is a polynomial in s of degree $d = n - |J|$.

We also note that for two pairs (J, τ) and (J', τ'), we have

$$C(J, \tau) \cap C(J', \tau') = \begin{cases} \emptyset \text{ if } J \cap J' \neq \emptyset \text{ and } \tau(j) \neq \tau'(j) \text{ for some } j \in J \cap J' \\ C(J \cup J', \tau \cup \tau') \text{ otherwise} \end{cases}$$

Claim: There exists a finite collection $\mathcal{J}$ of pairs (J, τ) such that

$$C(I) = \bigcup_{(J,\tau) \in \mathcal{J}} C(J, \tau)$$

For $\beta \in \mathbb{N}^n$ let $C(\beta) = \{\alpha \in \mathbb{N}^n : X^\beta \nmid X^\alpha\}$. Then $C(I) = \bigcap C(\beta^{(i)})$. We first show that $C(\beta)$ can be covered by some $C(J, \tau)$. Indeed, $\alpha \in C(\beta)$ if and only if there exists an $i \in \{1, \ldots, n\}$ such that $\alpha_i < \beta_i$. Hence,

$$C(\beta) = \bigcup_{i=1}^{n} \bigcup_{t_i=0}^{\beta_i - 1} \{(\alpha_1, \ldots, \alpha_n) : \alpha_i = t_i\} = \bigcup_{i=1}^{n} \bigcup_{t_i} C(\{t_i\}, \tau : i \to t_i)$$

Now, the claim follows from

$$C(I) = \bigcap_{i=1}^{m} C(\beta^{(i)}) = \bigcap_{i=1}^{m} \bigcup_{(J,\tau)} C(J, \tau) = \bigcup_{(J,\tau),(J',\tau')} (C(J, \tau) \cap C(J', \tau')) = \bigcup_{(J,\tau) \in \mathcal{J}} C(J, \tau)$$

The theorem now follows from the inclusion-exclusion principle: If $A_1, \ldots, A_k$ are finite sets then

$$|A_1 \cup A_2 \cup \ldots \cup A_k| = \sum_{r=1}^{k} \sum_{1 \leq i_1 < \ldots < i_r \leq m} (-1)^{r-1} |A_{i_1} \cap \ldots \cap A_{i_r}|$$

Applying this to $C(I)$ written as a union of $C(J, \tau)$ gives the desired polynomial $HP_I(t)$. Moreover, the degree can be computed as

$$\deg HP_I(t) = \max\{n - |J| : \exists (J, \tau) \text{ with } C(J, \tau) \subset C(I)\}$$

□

▶ Let $I = (Y - X^2, Z - X^3) \subset k[X, Y, Z]$. Using $\leq_{grlex}$, one can show that $G = \{X^2 - Y, XY - Z, XZ - Y^2, Y^3 - Z^2\}$ is a Gröbner basis. For example, here is how to do it in Macaulay 2:

```
R = QQ[x,y,z, MonomialOrder => GLex];
I = ideal (y-x^2,z-x^3);
gens gb I
```

Thus, $\mathfrak{in}(I) = \{X^2, XY, XZ, Y^3\}$. From which, we deduce that $C(I) = \{1, X, Y, Z\} \cup \{Z^s, YZ^{s-1}, Y^2Z^{s-2}\}_{s \geq 2}$ and $HP_I(t) = 3t + 1$.

The Hilbert polynomial provides one computable way of defining the dimension of a variety:

Definition 4.17. *Let $V = \mathcal{V}(I)$ be an affine variety defined by an ideal $I \subset k[X_1, \ldots, X_n]$. If $V \neq \emptyset$, then $\mathcal{I}(V) \neq k[X_1, \ldots, X_n]$ and $HP_{\mathcal{I}(V)} \neq 0$. We define*

$$\dim(V) \coloneqq \deg HP_{\mathcal{I}(V)}(t).$$

◁ Suppose that V is a linear space, that is

$$V = \mathcal{V}(\{f_j = \sum_{i=1}^{n} a_{ij} X_i : 1 \leq j \leq m\})$$

Show that $\dim_k V = \dim V = \deg HP_{\mathcal{I}(V)}(t)$.

The previous exercise gives a justification for the definition of the dimension as it generalizes the notion of dimension for linear spaces. Here is a more geometric justification that applies in general.

Corollary 4.18. *Let $I \subset k[X_1, \ldots, X_n]$ be a proper ideal.*

$$\deg HP_I(t) = \max\{0 \leq d \leq n : \textit{There exist } 1 \leq i_1 < i_2 \ldots < i_d \leq n \textit{ such that } I \cap k[X_{i_1}, \ldots, X_{i_d}] = \{0\}\}$$

In other words, this means that there exists d "algebraically independent" directions to project $V(I)$ by restricting $(X_{i_1}, X_{i_2}, \ldots, X_{i_d})$ to $V(I) \subset k^n$ and up to linear change of co-ordinates (for k infinite) one can further show that the projection to k^d is onto with finite fibers (this is the topic of Noether normalization theorem that we will see later).

Proof. In the proof of the Theorem 4.16, we have seen that

$$\deg HP_I(t) = \max\{n - |J| : \exists (J, \tau) \text{ with } C(J, \tau) \subset C(I)\}$$

We will show first that if (J, τ) is a pair such that $C(J, \tau) \subset C(I)$ then $I \cap k[X_j : j \notin J] = \{0\}$. Suppose that there exists $f \in I \cap k[X_j : j \notin J]$. Then $LT(f) \in LT(I) \cap k[X_j | j \notin J]$. Let us write $LT(f) = aX^\alpha$, then $\alpha_j = 0$ for all $j \in J$. Thus, $\gamma + \alpha \in C(J, \tau) \subset C(I)$ for all $\gamma \in C(J, \tau)$. On the other hand, $X^{\gamma+\alpha} = X^\gamma LT(f) \in \mathfrak{in}(I)$. But, this contradicts with $\gamma + \alpha \in C(I)$.

Conversely, suppose that we have a sequence $1 \leq i_1 < \ldots < i_d \leq n$ such that $I \cap k[X_{i_1}, \ldots, X_{i_d}] = 0$. We will show that $d \leq \deg HP_I(t)$. Consider the ring homomorphisms

$$k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] \to k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/I.$$

By assumption, the kernel of the composition is trivial. It follows that if we fix $s \geq 0$, the composition of the k-linear maps

$$k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]_{\leq s} \to k[X_1, \ldots, X_n]_{\leq s} \to k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}$$

is also injective. Hence, $\dim_k k[X_{i_1}, \ldots, X_{i_d}]_{\leq s} \leq HF_I(s)$. Hence,

$$HF_I(s) \geq \binom{d+s}{s} = \frac{1}{d!}(s^d + \ldots),$$

Since we have $HF_I(s) = HP_I(s)$ for s sufficiently large, it follows that $d \leq \deg HP_I(t)$. □

Here is how you may compute Hilbert polynomial in Macaulay 2:

```
R = QQ[x,y,z,w]
I = ideal(y-x^2,z-x^3)
inI = ideal leadTerm I
hilbertPolynomial(inI, Projective=>false)
```

This code computes the Hilbert polynomial of $I = (Y - X^2, Z - X^3) \subset \mathbb{Q}[X, Y, Z]$. However, we added one more variable to the ring in the code. This is because by default Macaulay 2 computes projective Hilbert polynomial of a homogeneous ideal. Our trick of adding one more variable "homogenises" the initial ideal. It is easy to see that computing the projective Hilbert polynomial homogenised ideal gives the same answer as the Hilbert polynomial of the original ideal.

4.5 Nullstellensatz : Theorem of zeroes

Recall that $k[X]$ is a PID, hence any ideal $I = (f)$ for some $f \in k[X]$. The affine variety $\mathcal{V}(I)$ is thus simply the set of roots of f. If k is algebraically closed, then every nonconstant polynomial f has a root (by the fundamental theorem of algebra). Therefore, $\mathcal{V}(I) = 0$ if and only if $I = k[X]$: Any proper ideal corresponds to a non-empty affine variety. The assumption k is algebraically closed is absolutely necessary as the example $I = (X^2 + 1) \in \mathbb{R}[X]$ gives the empty variety.

An important result of Hilbert, known by the German name **Nullstellensatz** (literally translates to "zero places theorem") says that the same statement holds in the case of a polynomial ring with many variables.

Theorem 4.19. *(Weak Nullstellensatz) If k is algebraically closed, and $I \neq k[X_1, \ldots, X_n]$ is a proper ideal, then $\mathcal{V}(I) \neq \emptyset$.*

There are various equivalent formulations (and proofs) of the Weak Nullstellensatz as well as a Strong Nullstellensatz. We will cover some of these. The approach that I found most worthwhile to prove goes via Noether normalization lemma which is an important structural result for finite-dimensional algebras over k. We will spend some time developing the notion of "integral dependence" before giving a proof of the Nullstellensatz. The key definition is the following.

Definition 4.20. *Suppose A and B are commutative rings such that $A \subset B$. We say that $b \in B$ is* **integral** *over A if there exists $m \geq 1$ and $a_0, a_1, \ldots, a_{m-1} \in A$ such that*

$$b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0 = 0$$

We say that B is integral over A if all elements of B are integral over A.

In other words, an element b of B is said to be integral over A if there exists a **monic** polynomial f in $A[X]$ such that $f(b) = 0$.

▶ Let $A = \mathbb{Z}$ and $B = \mathbb{Q}$. The only integral elements of B over A are just $\mathbb{Z}$.

▶ Let $A = \mathbb{Z}$ and $B = \mathbb{Q}(i)$. The only integral elements of B over A are Gaussian integers $\mathbb{Z}(i)$.

▶ Let $A = \mathbb{Z}(\sqrt{-3})$ and $B = \mathbb{Q}(\sqrt{-3})$. The integral elements of B over A are Eisenstein integers $\mathbb{Z}[\omega]$.

More generally, in algebraic number theory, one studies the **ring of integers**, denoted by $\mathcal{O}_K$, of a number field K (a finite extension of $\mathbb{Q}$) defined as

$$\mathcal{O}_K = \{b \in K : b \text{ is integral over } \mathbb{Z}\}.$$

The fact that this is a ring is not quite obvious from the definition of integral elements, but follows from the following characterisation.

Lemma 4.21. *Suppose $b \in B$. The following conditions are equivalent:*

i. b is integral over A.

ii. $A[b] \coloneqq \{f(b) : f \in A[X]\}$ is finitely generated over A as a module.

iii. There exists a subring $C \subset B$ such that $A[b] \subset C$ and C is finitely generated over A as a module.

We will need Cramer's rule from linear algebra which we recall for convenience. Let $M \in M_n(A)$ be an n-by-n matrix with entries in A and $Mx = y$ is a set of n linear equations, where x and y are column vectors. Write $M = [m_1\ m_2\ \ldots\ m_n]$ where m_i are column vectors. Then the n linear equations can be written as

$$x_1 m_1 + x_2 m_2 + \ldots + x_n m_n = y.$$

We define new n-by-n matrices $M_j = [m_1\ m_2\ \ldots\ m_{j-1}\ y\ m_{j+1}\ \ldots\ m_n]$. Then,

$$\det M_j = \sum_{i=1}^{n} x_i \det[m_1\ m_2\ \ldots\ m_{j-1}\ m_i\ m_{j+1}\ \ldots\ m_n] = x_j \det M$$

Proof. (of Lemma 4.21) *i.* implies *ii.* : By the hypothesis, we have a monic polynomial $g \in A[X]$ such that $g(b) = 0$. Given $f \in A[X]$, we can divide by g (as g is monic!) and write

$$f = gh + r, \text{ with } h, r \in A[X]$$

where $r = 0$ or $deg(r) < deg(g) = m$. Then, $f(b) = g(b)h(b) + r(b)$. Hence, $A[b] = \{r(b) : r = 0 \text{ or } deg(r) < m\} = A \cdot 1 + A \cdot b + \ldots + A \cdot b^{m-1}$.

ii. implies *iii.* : Trivial. Take $C = A[b]$.

iii. implies *i.* : We have $C = Ac_1 + Ac_2 + \ldots + Ac_n$ with $c_i \in C$. Since $b \in C$ and C is a ring, we can write

$$bc_i = \sum_{j=1}^{n} a_{ij}c_j \text{ for } a_{ij} \in A$$

Consider the n-by-n matrix N with entries a_{ij} and x be the column vector with entries c_i. Then, we have $Nx = bx$ or equivalently $(N - bI_n)x = 0$. By Cramer's rule applied to $M = N - bI_n$, we get the equations

$$c_i \det(N - bI_n) = 0, \text{ for all } i.$$

($\det M_j = 0$ since $y = 0$.) On the other hand, $1 \in C$, hence there exist $a_i \in A$ such that $1 = \sum_{i=1}^{n} a_i c_i$. It follows that

$$\det(N - bI_n) = \sum_{i=1}^{n} a_i c_i \det(N - bI_n) = 0.$$

Let $p(X) = \det(N - XI_n)$. We have $p(X) \in A[X]$ is a monic polynomial satisfying $p(b) = 0$. □

For example, consider the ring $B = k[X, Y]/(X^2 - Y^2)$ and its subring isomorphic to $A = k[Y]$ generated by $Y + (X^2 - Y^2)$. It is easy to see B is finite as an A-module. Indeed, $B = A \cdot 1 + A \cdot X$. Hence, B is integral over A.

Corollary 4.22. *Let A and B be commutative rings with $A \subset B$.*

(a) Suppose $B = A[b_1, \ldots, b_n]$ with $b_i \in B$ such that b_i are integral over $A[b_1, \ldots, b_{i-1}]$ for all i. Then B is integral over A and B is finitely generated as an A-module.

(b) The integral closure $\overline{A}_B := \{b \in B : b \text{ integral over} A\}$ is a subring of B.

(c) Let C be a ring with $A \subset C \subset B$ such that C is integral over A and B is integral over C, then B is integral over A.

(d) Let B be integral over A. If B is a field, then A is also a field. Conversely, if A is a field, and B is an integral domain, then B is also a field.

Proof. (a) is immediate by recursion.

(b) Given $b, b' \in B$ integral over A from (a) we get $A[b, b'] \subset B$ is finitely generated over A and so integral over A. 5

(*c*) Let $b \in B$ integral over C, then we have an equation

$$b^m + c_{m-1}b^{m-1} + \ldots + c_1 b + c_0 = 0 \text{ for some } c_0, \ldots, c_{m-1} \in C$$

Let $C' = A[b, c_0, \ldots, c_{m-1}] \subset B$. The ring $A[c_0, \ldots, c_{m-1}]$ is integral over A, and by part (a), C' is integral over A. Hence, b is integral over A.

(*d*) Let B be a field, and $a \in A$ be a nonzero element. Then $a^{-1} \in B$. We want to show that $a^{-1} \in A$. Since B is integral over A, there is a relation

$$a^{-n} + c_{n-1}a^{-n+1} + \ldots + c_0 = 0, \text{ with } \ c_i \in A$$

Then, we have $a^{-1} = -(c_{n-1} + c_{n-2}a + \ldots + c_0 a^{n-1}) \in A$.

Conversely, suppose A is a field and B is an integral domain. Let $b \in B$ a non-zero element. We have an equation

$$b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0 = 0 \text{ with } \ a_i \in A$$

Since B is an integral domain, we can assume that $a_0 \neq 0$. Then,

$$b^{-1} = -a_0^{-1}(b^{m-1} + a_{m-1}b^{m-2} + \ldots + a_1).$$

□

Definition 4.23. *A is said to be* **integrally closed** *in B if $\overline{A}_B = A$. Assuming that A is an integral domain, we can see A embedded in its field of fractions: $A \subset Frac(A)$. We say that an integral domain is* **normal** *if it is integrally closed in its field of fractions. If A is an integral domain, the integral closure of A in $Frac(A)$ is called the* **normalisation** *of A.*

▶ The ring $k[X_1, \ldots, X_n]$ is normal.

◁ More generally, a ring which is a UFD is normal.

◁ The ring $A = k[x, y]/(y^2 - x^3)$ is not normal. Indeed, the element $t = y/x \in Frac(A)$ satisfies the monic equation $t^2 - x = 0$ (and $t^3 - y = 0$). Show that the normalisation of A is isomorphic to $k[t]$.

Macaulay 2 can tell you whether a ring is normal, and compute the normalisation if not.

```
R = QQ[x,y]/(y^2-x^3)
isNormal R
S = integralClosure R
describe S
```

Definition 4.24. *Let k be a field. We say that A is a k-algebra if*

(a) A is a vector space over k

(b) A is a commutative ring (with unity)

(c) $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $a, b \in A$ and $\lambda \in k$.

Standard example of a k-algebra is the polynomial ring $k[X_1, \ldots, X_n]$ or more generally a quotient ring $A = k[X_1, \ldots, X_n]/I$ by an ideal I. We say that a k-algebra A is **finitely generated** if A is generated by a finitely many number of elements as an algebra. More precisely, there exist elements $a_1, \ldots, a_n \in A$ such that $A = \{f(a_1, \ldots, a_n) : f \in k[X_1, \ldots, X_n]\}$. We write $A = k[a_1, \ldots, a_n]$. In this case, we have a surjective homomorphism

$$\pi : k[X_1, \ldots, X_n] \to A$$

given by $\pi(X_i) = a_i$ and A is isomorphic to $k[X_1, \ldots, X_n]/\ker(\pi)$.

More generally, if $A \subset B$ are commutative rings. We say that B is finitely generated as an A-algebra if B is isomorphic to $A[X_1, \ldots, X_n]/I$ for some n and ideal I in which case we can write $B = A[b_1, \ldots, b_n]$ for some $b_i \in B$. It is important not to confuse this with the similar sounding statement that says that B is a finitely generated A-module.

▶ Let $A \subset B$ be commutative rings. It follows easily from Lemma 4.21 that B is finitely generated as an A-module if and only if B is finitely generated as an A-algebra and integral over A.

We say that $a_1, \ldots, a_n$ are **algebraically independent** if there is no non-zero polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(a_1, \ldots, a_n) = 0$. This is equivalent to the injectivity of the homomorphism π.

Theorem 4.25. *(Noether normalisation[4] lemma) Let A be a finitely generated k-algebra. Then there exists $a_1, \ldots, a_d \in A$ such that*

- *$\{a_1, \ldots, a_d\}$ are algebraically independent.*
- *$A \supset k[a_1, \ldots, a_d]$ is integral.*

In other words, a finitely generated extension $k \subset A$ can be written as a composition

$$k \subset k[a_1, \ldots, a_d] \subset A$$

where the first extension is "free" (given by a polynomial algebra over k) and the second one is "finite" (finitely generated extension as a module).

◁ Find a polynomial subalgebra of $A = \mathbb{Q}[X, Y, Z]/(XY - Z^2)$ over which A is integral.

Proof. The original proof of E. Noether assumes k is an infinite field. Let's do that and later I will explain Nagata's modification of the proof which doesn't have this extra assumption.

Write $A = k[b_1, \ldots, b_n]$ for some $b_i \in A$. Suppose that $b_1, \ldots, b_n$ are algebraically dependent over k, and let $f(b_1, \ldots, b_n) = 0$ be a relation, where $f \in k[X_1, \ldots, X_n]$ is a non-constant polynomial. Write m for the degree of f, and let $f_m(X_1, \ldots, X_n)$ be the homogeneous part of f of degree m. Take $c_1, \ldots, c_{n-1} \in k$ such that $f_m(c_1, \ldots, c_{n-1}, 1) \neq 0$. (It is at this step that we use k is

[4] Although closely related, the usage of the word "normalisation" here does not agree with the normalisation defined above as the integral closure of an integral domain in its field of fractions. Both usages are standard.

infinite.) We now make a substitution by letting $y_i = x_i - c_i x_n$ for $i = 1, \ldots, n-1$. Then, we have

$$\begin{aligned} 0 = f(x_1, \ldots, x_n) &= f(y_1 + c_1 x_n, y_2 + c_2 x_n, \ldots, y_{n-1} + c_{n-1} x_n, x_n) \\ &= f_m(c_1, c_2, \ldots, c_{n-1}, 1) x_n^m + g_1 x_n^{m-1} + \ldots + g_m \end{aligned}$$

where $g_i \in k[y_1, \ldots, y_{n-1}]$ so that x_n is integral over $k[y_1, \ldots, y_{n-1}]$. Then, it follows that $x_i = y_i + c_i x_n$ are also integral over $k[y_1, \ldots, y_{n-1}]$. Therefore, A is integral over $k[y_1, \ldots, y_{n-1}]$. The result now follows by induction on n.

If k is finite (Nagata): We modify the substitution to the following: Choose $r_1, \ldots, r_{n-1} \in \mathbb{N}$ and make the substitution $y_i = x_i - x_n^{r_i}$. Then, for a monomial X^α we have

$$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n} = (Y_1 + X_n^{r_1})^{\alpha_1} (Y_2 + X_n^{r_2})^{\alpha_2} \ldots (Y_{n-1} + X_n^{r_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n} = X_n^{N(\alpha)} + \sum_{r=0}^{N(\alpha)} g_i^\alpha X_n^i$$

where $N(\alpha) = (\sum_{i=1}^{n-1} r_i \alpha_i) + \alpha_n$ and $g_i^\alpha \in k[y_1, \ldots, y_{n-1}]$. Hence, $f = \sum_\alpha a_\alpha X^\alpha = \sum_\alpha a_\alpha (X_n^{N(\alpha)} + \sum_i g_i^\alpha X_n^i)$ Now, we want to choose r_i so that the function $\alpha \to N(\alpha)$ is injective so that no cancellation among top powers of X_n take place. We can ensure this by picking $r \geq \alpha_i$ for all $\alpha = (\alpha_1, \ldots, \alpha_n)$ with $a_\alpha \neq 0$ and letting $r_i = r^{n-i}$ so that $N(\alpha) = r^{n-1}\alpha_1 + r^{n-2}\alpha_2 + \ldots + r\alpha_{n-1} + \alpha_n$. Then, we have

$$f = a X_n^N + \sum_{i=1}^{N-1} g_i X_n^i \text{ with } g_i \in k[Y_1, \ldots, Y_{n-1}], 0 \neq a \in k$$

where $N = \max\{N(\alpha) : a_\alpha \neq 0\}$. The rest of the proof works as before. □

Although we do not give a proof here, it is helpful for the intuition to remark on the geometric meaning of Noether's normalisation. Let $V = \mathcal{V}(I)$ be an affine variety and $A = k[X_1, \ldots, X_n]/\mathcal{I}(V)$ be the finitely generated k-algebra of polynomial functions on V. Noether normalisation gives a subring $k[Y_1, \ldots, Y_d] \subset A$ over which A is integral. For k algebraically closed, this implies that the corresponding map of varieties $\pi : V \to k^d$ is onto with finite fibres (the proof of this claim uses Hilbert's Nullstellensatz as well as the lying-over theorem for integral extensions that we will establish later in the course).

Here is how you can do Noether normalisation in Macaulay 2:

```
loadPackage "NoetherNormalization"
R = Z/2 [x,y]
I = ideal(x*y)
(f,J,X) = noetherNormalization I
-- The computations performed use a random linear change of coordinates.
-- This returns f an automorphism of R, J the image of I under f, and
-- X a list of variables which are algebraically independent in R/J.
-- In our example, we get f: (x,y) \to (x, x+y) , J = x^2+xy, X = {y}
```

Thus, we see that $k[X,Y]/(XY) \simeq k[X,Y]/(X^2+XY)$ is an integral extension of $k[Y]$ obtained by adjoining X which satisfies the monic polynomial $X^2+XY=0$.

◁ Show that an algebraically closed field k is infinite. (Suppose that k is finite with n elements and consider the polynomial $X^n - X + 1$.)

It can be shown that the number d that appeared in Noether normalisation lemma is equal to the maximal number of elements in A that are algebraically independent over k (see Corollary 4.27 that implies this when A is an integral domain, and the general case follows from this using Corollary 4.36). This is another way to measure the dimension as the following proposition shows.

Proposition 4.26. *Let $V \subset k^n$ be an affine variety, $I = \mathcal{I}(V)$ and $A = k[X_1,\dots,X_n]/I$ the co-ordinate ring of V. Then, the maximal number of algebraically independent elements in A is equal to* $\dim V = \deg HP_I(t)$.

Proof. Let us first show that if $d = \dim V$, we can find d elements in A which are algebraically independent. By Corollary 4.18, we know that

$$d = \max\{0 \le d \le n : \text{There exist } 1 \le i_1 < i_2 \dots < i_d \le n \text{ such that } I \cap k[X_{i_1},\dots,X_{i_d}] = \{0\}\}$$

Denote by $\overline{\ }: k[X_1,X_2,\dots,X_n] \to A$ the canonical projection map. Since $I \cap k[X_{i_1},\dots,X_{i_d}] = \{0\}$, the map $k[X_{i_1},X_{i_2},\dots,X_{i_d}] \to A$ is injective. Hence, $\overline{X}_{i_1},\overline{X}_{i_2},\dots,\overline{X}_{i_d}$ are algebraically independent in A.

Conversely, let $\overline{f}_1,\overline{f}_2,\dots,\overline{f}_d$ be algebraically independent elements in A. Let N be the largest of the total degress of $f_1,f_2,\dots,f_d$. We construct a map

$$k[Y_1,Y_2,\dots,Y_d]_{\le s} \to k[X_1,X_2,\dots,X_n]_{\le Ns}/I_{\le Ns}$$

given by sending $F(y_1,y_2,\dots,y_d) \in k[Y_1,Y_2,\dots,Y_d]_{\le s}$ to $\overline{F(f_1,f_2,\dots,f_d)} \in k[X_1,\dots,X_n]_{\le Ns}/I_{\le Ns}$. We claim that this map is injective. Indeed, suppose that $F(f_1,f_2,\dots,f_d) \in I_{\le Ns}$. This means that $\overline{F(f_1,f_2,\dots,f_d)} = F(\overline{f_1},\overline{f_2},\dots,\overline{f_d}) = 0$ in A. But since $\overline{f}_1,\dots,\overline{f}_d$ are algebraically independent, it follows that $F=0$. Therefore,

$$HF_I(Ns) = \dim_k(k[X_1,X_2,\dots,X_n]_{\le Ns}/I_{\le Ns}) \ge \dim[Y_1,Y_2,\dots,Y_d]_{\le s} = \binom{s+d}{d} = \frac{1}{d!}s^d + \dots$$

Thus it follows that $HP_I(s)$ must have degree at least d, as required. □

▶ Consider the k-algebra $A = k[X,Y,Z]/(XY,XZ)$. We observe that both of the sets $\{X\}$ and $\{Y,Z\}$ are maximal algebraically independent subsets over k, that is, we cannot add more elements to these sets keeping them algebraically independent, so unlike in the case of field extensions, not all maximal subsets consisting of algebrically independent subsets have the same cardinality.

We can remedy this situation by restricting our attention to integral domains $A = k[X_1,\dots,X_n]/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal. Then, we can consider the field of fractions of A, $K = Frac(A)$, and

it is easy to see that if $\{a_1, \ldots, a_d\}$ is a maximal set of algebraically independent elements in A, then we have the corresponding field extensions

$$k \subset k(a_1, \ldots, a_d) \subset K$$

where the first extension is purely transcendental and the second one is an algebraic extension. Therefore, the cardinality of maximal algebraically independent subsets is well-defined and equal to the transcendence degree of the field extension $k \subset K$ (recall that transcendence degree of a field extension $k \subset K$ is defined as the largest cardinality of an algebraically independent subset in K over k). Combining this discussion with Proposition 4.26 gives us a field theoretical characterisation of dimension.

Corollary 4.27. *Let $V \subset k^n$ be an affine variety, and suppose that $\mathfrak{p} = \mathcal{I}(V)$ is a prime ideal. Then $\dim V$ is equal to the transcendence degree of the field extension $k \subset Frac(A)$, where $A = k[X_1, \ldots, X_n]/\mathcal{I}(V)$.*

We next turn to one of the most important theorems in this course.

Theorem 4.28. *(Nullstellensatz - weak version) Suppose that k is algebraically closed. Then, the maximal ideals of $k[X_1, \ldots, X_n]$ are exactly of the form*

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n), \text{ where } a_i \in k.$$

Furthermore, if $I \subset k[X_1, \ldots, X_n]$ is a proper ideal, then $\mathcal{V}(I) \neq \emptyset$..

Proof. Let I be an ideal of the form $I = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ with $a_i \in k$. Consider the homomorphism $\sigma : k[X_1, X_2, \ldots, X_n] \to k$ given by sending $X_i \to a_i$. Then $I \subset \ker(\sigma)$. Moreover $\ker(\sigma)$ is a maximal ideal since $k[X_1, \ldots, X_n]/\ker(\sigma) \simeq k$. Conversely, let $f \in \ker(\sigma)$. Choose a monomial order and apply division with remainder to write

$$f = h_1(X_1 - a_1) + h_2(X_2 - a_2) + \ldots + h_n(X_n - a_n) + r, \text{ with } r \in k$$

Then $0 = f(a_1, a_2, \ldots, a_n) = r$ hence, $f \in I$. Thus, we have $I = \ker(\sigma)$.

Conversely, suppose $I \subset k[X_1, \ldots, X_n]$ be a maximal ideal. Then $A = k[X_1, \ldots, X_n]/I$ is a field that is a finitely generated k-algebra. Applying Noether's normalisation, we can find $u_1, \ldots, u_d \in A$ which are algebraically independent such that the extension $A \supset k[u_1, \ldots, u_d]$ is integral. But, A is a field, therefore $k[u_1, \ldots, u_d]$ is a field by Corollary 4.22 (d). Now, $k[u_1, \ldots, u_d]$ is a polynomial algebra that is a field, hence it follows that $d = 0$. In other words, $A \supset k$ is an integral extension. This means that $A \supset k$ is an algebraic extension of fields but k is algebraically closed, hence $A = k$. Thus, if we define a_i to be the image of $_i$ under the isomorphism $k[X_1, \ldots, X_n]/I \simeq k$, we see that $X_i - a_i \in I$. Hence,

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subset I$$

but $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ is a maximal ideal, hence

$$I = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n).$$

In particular, if I is a proper ideal, by Proposition 2.4 (!) there exists a maximal ideal containing I, that is, there exist $a_1, a_2, \ldots, a_n$ such that

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \supset I$$

Hence, applying $\mathcal{V}$, we see that $(a_1, a_2, \ldots, a_n) \in \mathcal{V}(I)$. □

▶ In the course of the proof, we saw a proof of the following statement:

Lemma 4.29. *(Zariski's lemma) Suppose that a field K is a finitely generated as an algebra over a field k, then it is finitely generated as a module.*

In other words, for a field extension the two notions of finitely generated coincide. Our proof of this used Noether normalisation. There are other direct proofs of Zariski's lemma which can be used to give a different proof of the Nullstellensatz.

In the end of the proof, I sneakily appealed to Proposition 2.4 whose proof uses Zorn's lemma to show that every proper ideal is contained in a maximal ideal. Most books on commutative algebra do this. Of course, it is rather unsatisfactory[5]. Let us remark that Proposition 2.4 was proved for a general commutative ring. The above theorem is concerned with the ring $k[X_1, \ldots, X_n]$ which we know is Noetherian from Theorem 4.1 and so the existence of a maximal ideal containing a proper ideal can be proved directly (just form an ascending chain out of ideals containing I and appeal to Noetherian property to show that such a chain stabilises). However, this too uses a countable version of Axiom of Choice since we make infinitely many choices as we form the ascending chain.

For the true constructivists, let us now give a constructive proof following the nice article by Arrondo [7] which avoids any choice.

Theorem 4.30. *(Nullstellensatz without choice) Let k be any field. Any proper ideal $I \subset k[X_1, X_2 \ldots, X_n]$ is contained in a maximal ideal $\mathfrak{m}$.*

We first prove a lemma that we will use for the inductive step of the proof.

Lemma 4.31. *Let $I \subset k[X_1, \ldots, X_n]$ a proper ideal containing a polynomial g that is monic in X_n, thus*

$$g = X_n^d + X_n^{d-1} g_{d-1} + \ldots + X_n g_1 + g_0 \text{ with } g_i \in k[X_1, \ldots, X_{n-1}]$$

If $\mathfrak{m}' \subset k[X_1, \ldots, X_n]$ is a maximal ideal containing $I' = I \cap k[X_1, \ldots, X_{n-1}]$. Then, the ideal $I + (\mathfrak{m}') \subset k[X_1, \ldots, X_n]$ is proper.

Proof. Suppose for contradiction there exist $f \in I$ and $f' \in (\mathfrak{m}')$ such that $f + f' = 1$ or equivalently $f - 1 \in (\mathfrak{m}')$. Let us write

$$f = f_e X_n^e + f_{e-1} X_n^{e-1} + \ldots + f_1 X_n + f_0 \text{ with } f_i \in k[X_1, X_2, \ldots, X_{n-1}].$$

[5] There are people out there who build machines using polynomial equations.

We have that $f_0 - 1, f_1, f_2, \ldots, f_e \in \mathfrak{m}'$. Viewing both f and g as in $k[X_1, \ldots, X_{n-1}][X_n]$, we can consider their **resultant** with respect to the variable X_n. This is the polynomial in $k[X_1, \ldots, X_{n-1}]$ given by the determinant

$$R = \begin{vmatrix} f_0 & f_1 & \ldots & f_e & 0 & 0 & \ldots & 0 \\ 0 & f_0 & \ldots & f_{e-1} & f_e & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & f_0 & f_1 & \ldots & f_{e-1} & f_e \\ g_0 & g_1 & \ldots & g_{d-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{d-2} & g_{d-1} & 1 & 0 \ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{d-1} & 1 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} d \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} e \text{ rows} \\ . \end{matrix}$$

First note that R belongs to I. To see this, multiply the second column by X_n, third column by X_n^2 , and so on until the last column which is to be multiplied by X_n^{d+e-1} and add all these to the first column. This doesn't change the determinant. The resulting matrix then is as follows:

$$R = \begin{vmatrix} f & f_1 & \ldots & f_e & 0 & 0 & \ldots & 0 \\ X_n f & f_0 & \ldots & f_{e-1} & f_e & 0 & \ldots & 0 \\ & \ddots & & & & & & \\ X_n^{d-1} f & \ldots & 0 & f_0 & f_1 & \ldots & f_{e-1} & f_e \\ g & g_1 & \ldots & g_{d-1} & 1 & 0 & \ldots & 0 \\ X_n g & g_0 & \ldots & g_{d-2} & g_{d-1} & 1 & 0 \ldots & 0 \\ & & \ddots & & & & \ddots & \\ X_n^{e-1} g & \ldots & 0 & g_0 & g_1 & \ldots & g_{d-1} & 1 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} d \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} e \text{ rows} \\ . \end{matrix}$$

Now, expanding the determinant by the first column shows that R is a linear combination of f and g. Thus, $R \in I \cap k[X_1, \ldots, X_n] = I' \subset \mathfrak{m}'$. On the other hand, in $k[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$, the original matrix representing R becomes a lower triangular matrix (since $f_0 - 1, f_1, \ldots, f_{n-1} \in \mathfrak{m}'$), hence $R = 1 \in k[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$, that is $R \notin \mathfrak{m}'$, which is a contradiction. □

Proof. (of Theorem 4.30) We argue by induction on n. The case $n = 1$ is obvious since $k[X]$ is a PID. Any ideal is of the form (f) and any irreducible factor of f generates a maximal ideal containing (f). Suppose $n > 1$. Let $g \in I$ be a non-constant polynomial, as in the proof of the Noether normalization lemma, we can find change of co-ordinates if necessary such g is monic with respect to X_n. So, we can assume that I contains such a g. Now, consider $I' = I \cap k[X_1, \ldots, X_{n-1}]$. Since I is proper, $1 \notin I$, hence I' is also proper. By induction hypothesis, there exists a maximal ideal $\mathfrak{m}'$ containing I'. Let k' be the field $k' = k[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$. Consider the surjective homomorphim $\pi : k'[X_n] \to k[X_1, X_2, \ldots, X_n]/(I + (\mathfrak{m}'))$. We have the isomorphism of rings

$$k'[X_n]/\mathrm{Ker}(\pi) \simeq k[X_1, X_2, \ldots, X_n]/(I + (\mathfrak{m}'))$$

Now, by the previous lemma $I+(\mathfrak{m}')$ is a proper ideal, hence $\mathrm{Ker}(\pi)$ is a proper ideal. As $k'[X_n]$ is a PID, we have a maximal ideal containing $\mathrm{Ker}(\pi)$, which by the above isomorphism goes to a maximal ideal $\mathfrak{m}$ containing $I+(\mathfrak{m}')$ hence also containing I. □

There you go; a proof without the axiom of choice. From now on, as long as we work with polynomial rings with field coefficients and their quotients, you can rest assured that every ideal has a maximal ideal containing it.

Theorem 4.32. *(Nullstellensatz - Strong form) Suppose that k is algebraically closed. $I \subset k[X_1,\ldots,X_n]$ is an ideal. Then*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

Proof. $I \subset \mathcal{I}(\mathcal{V}(I))$ is obvious. Let's show $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$. Let $f \in \sqrt{I}$. This means that there exists $\ell \geq 1$ such that $f^\ell \in I \subset \mathcal{I}(\mathcal{V}(I))$. Hence, $f^\ell(x_1,\ldots,x_n) = 0$ for all $(x_1,\ldots,x_n) \in \mathcal{V}(I)$. But then, $f(x_1,\ldots,x_n) = 0$ for all $(x_1,\ldots,x_n) \in \mathcal{V}(I)$. Thus, $f \in \mathcal{I}(\mathcal{V}(I))$.

Conversely, let $I = (f_1,\ldots,f_s)$ with $f_i \in I$. Let $f \in k[X_1,\ldots,X_n]$ such that $f \in \mathcal{I}(\mathcal{V}(I))$. More explicitly, this means that if $(a_1,\ldots,a_n) \in k^n$ such that $f_i(a_1,\ldots,a_n) = 0$ for all i, then $f(a_1,\ldots,a_n) = 0$. We need to show that there exists an $\ell > 0$ and $h_1,\ldots,h_s \in k[X_1,\ldots,X_n]$ such that

$$f^\ell = \sum_{i=1}^{s} h_i f_i$$

For this, consider the polynomial ring $k[X_1,\ldots,X_n,Y]$ and the ideal $\tilde{I} = (f_1,\ldots,f_s,1-Yf) \subset k[X_1,\ldots,X_n,Y]$. We will show that $\tilde{I} = k[X_1,\ldots,X_n,Y]$. Indeed, if $\tilde{I}$ is a proper ideal, let $\mathfrak{m}$ be a maximal ideal containing $\tilde{I}$. By the weak version of the Nullstellensatz, there exist $a_1,a_2,\ldots,a_{n+1} \in k$ such that $\mathfrak{m} = (X_1-a_1, X_2-a_2,\ldots,X_n-a_n, Y-a_{n+1})$. Thus, for all $i = 1,\ldots s$, $f_i(a_1,\ldots,a_n) = 0$. Therefore, $f(a_1,\ldots,a_n) = 0$. But we also have $1-fY \in \mathfrak{m}$ which gives

$$1 - f(a_1,\ldots,a_n)a_{n+1} = 0$$

which contradicts the fact that $f(a_1,\ldots,a_n) = 0$. Hence, $\tilde{I} = k[X_1,\ldots,X_n,Y]$. Therefore, $1 \in \tilde{I}$. Hence, we can write

$$1 = \sum_{i=1}^{s} g_i f_i + (1-fY)g_{n+1}, \text{ for some } \; g_i \in k[X_1,\ldots,X_n,Y]$$

Now consider the homomorphism of rings sending $k[X_1,\ldots,X_n,Y] \to k(X_1,\ldots,X_n)$ by sending $X_i \to X_i$ for $1 \leq i \leq n$ and Y to $\frac{1}{f}$. We get the equation

$$1 = \sum_{i=1}^{s} g_i(X_1,\ldots,X_n,\frac{1}{f})f_i + 0$$

Choose ℓ sufficiently large so that $h_i(X_1,\ldots,X_n) \coloneqq f^\ell g_i(X_1,\ldots,X_n,\frac{1}{f}) \in k[X_1,\ldots,X_n]$ for all i. It follows that

$$f^\ell = \sum_{i=1}^{s} h_i f_i.$$

□

The most important consequence of the Nullstellensatz is that it establish a one-to-one inclusion reversing bijections

$$\text{affine varieties} \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} \text{radical ideals}$$

Corollary 4.33. *Let k be a field (not necessarily algebraically closed) and $I = (f_1, \ldots, f_s) \in k[X_1, \ldots, X_n]$. Then $f \in \sqrt{I}$ if and only if 1 belongs to the ideal $\tilde{I} = (f_1, \ldots, f_s, 1 - Yf) \in k[X_1, \ldots, X_n, Y]$.*

Proof. In the proof of Theorem 4.32, we saw that $1 \in \tilde{I}$ implies that $f \in \sqrt{I}$. Conversely, suppose $f \in \sqrt{I}$, then $f^\ell \in I$ for some $\ell > 0$. But we also have $1 - Yf \in \tilde{I}$, hence we can write

$$1 = Y^\ell f^\ell + (1 - Y^\ell f^\ell) = Y^\ell f^\ell + (1 - Yf) \cdot (1 + Yf + \ldots + Y^{\ell-1} f^{\ell-1}) \in \tilde{I}$$

□

This corollary gives an algorithmic way of determining whether $f \in \sqrt{I}$ for an ideal I which goes via computing a Gröbner basis for $(f_1, \ldots, f_s, 1 - Yf)$.

◁ Consider a 2-by-2 matrix M with entries X, Y, Z, W. If we then want to solve $M^2 = 0$, we get four equations and let's make that into an ideal $I = (X^2+YZ, XY+YW, XZ+WZ, W^2+YZ) \in k[X, Y, Z, W]$. Is I a radical ideal? Show that $\sqrt{I} = (X + W, XW - YZ)$.

You can also do this in Macaulay 2 :

```
R = QQ[x,y,z,w];
I = ideal (x^2+y*z,x*y+y*w,x*z+w*z,w^2+y*z);
I == radical I
radical I
```

◁ (Hard) Consider an n-by-n matrix X with entries $X_{i,j}$ for $1 \leq i, j \leq n$ and a n-by-n matrix Y with entries $Y_{i,j}$ for $1 \leq i, j \leq n$. Form an ideal $I \subset \mathbb{C}[X_{i,j}, Y_{i,j}]_{1 \leq i,j \leq n}$ generated by the entries of the matrix $XY - YX$. Is I a radical ideal? This is a well known open question. It is known that $\sqrt{I}$ is prime for all n but I is only known to be radical (or equivalently that I is known to be prime) for $n \leq 3$. We can verify this in Macaulay 2 as follows:

```
n=3
R = QQ[x_(1,1)..x_(n,n),y_(1,1)..y_(n,n)]
M = matrix table (n, n, (i,j) -> x_(i+1,j+1))
N = matrix table (n, n, (i,j) -> y_(i+1,j+1))
I = minors(1, M*N-N*M)
isPrime I
```

If you want to break your computer, you can set n to a higher value and run the same code.

Corollary 4.34. *Let k be algebraically closed. I a proper ideal in $k[X_1, \ldots, X_n]$. By the weak Nullstellensatz, we have that $V = \mathcal{V}(I) \subset k^n$ is non-empty.*

$$\dim V := \deg HP_{\mathcal{I}(V)}(t) = \deg HP_I(t)$$

Proof. $I \subset \mathcal{I}(V)$ hence $\deg HP_{\mathcal{I}(V)}(t) \leq \deg HP_I(t)$. To show the other inequality, suppose that $d = \deg HP_I(t)$. By Corollary 4.18, there exist $1 \leq i_1 < i_2 < \ldots < i_d \leq n$ such that $I \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = \{0\}$. It suffices to show that

$$\mathcal{I}(V) \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = \{0\}.$$

Let $f \in \mathcal{I}(V) \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$. Since $\mathcal{I}(V) = \sqrt{I}$, there exists $\ell \geq 1$ such that $f^\ell \in I$. On the other hand, $f \in k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$ implies that $f^\ell \in k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$ hence $f^\ell \in I \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$. Thus, $f = 0$. □

Corollary 4.35. *Let k be algebraically closed. $I \subset k[X_1, X_2, \ldots, X_n]$ be a proper ideal. Then, its radical $\sqrt{I}$ is the intersection of all maximal ideals containing I, that is,*

$$\sqrt{I} = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$$

Proof. The inclusion $\sqrt{I} \subset \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$ is true in any ring since $I \subset \sqrt{I} \subset \mathfrak{m}$ for any maximal ideal $\mathfrak{m} \supset I$. Now, let $f \in \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$. By the weak Nullstellensatz, all the maximal ideals containing I are of the form $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. Therefore, f vanishes on all $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. Hence, by the strong Nullstellensatz $f \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. □

The last corollary implies that the ring $k[X_1, \ldots, X_n]$ is a Jacobson ring - A ring R is called a **Jacobson ring** or **Hilbert ring** if every prime ideal is an intersection of maximal ideals. Equivalently, for every ideal I in R, the nilradical and the Jacobson radial in R/I coincide. A field is obviously a Jacobson ring. A generalization of Hilbert's Nullstellensatz states that any finitely generated algebra over a Jacobson ring is Jacobson. The last corollary should be contrasted with Proposition 2.7. Firstly, it says that it suffices to take only maximal ideals containing I, rather than all the prime ideals. Secondly, we have explicit descriptions of the maximal ideals containing I or equivalently maximal ideals in the ring $k[X_1, \ldots, X_n]/I$: They are in bijection with points of $\mathcal{V}(I)$.

On the other hand, we also have the following decomposition in terms of minimal prime ideals containing I.

Corollary 4.36. *Let k be algebraically closed and I a proper ideal in $k[X_1, \ldots, X_n]$. Then, there exist prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r \in k[X_1, \ldots, X_n]$ such that*

$$\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r.$$

Moreover,

$$\deg HP_I(t) = \deg HP_{\sqrt{I}}(t) = \max\{\deg HP_{\mathfrak{p}_i}(t) | 1 \leq i \leq r\}$$

Definition 4.37. *Let $V = \mathcal{V}(I)$ be an affine variety. V is said to be* **irreducible** *if V can not be written as a union $V = V_1 \cup V_2$ where $V_i \subsetneq V$ are affine varieties.*

Lemma 4.38. *Suppose $V = \mathcal{V}(I)$ is an irreducible affine variety. Then, $\mathcal{I}(V)$ is a prime ideal.*

Proof. Let $f, g \in k[X_1, \ldots, X_n]$ such that $fg \in \mathcal{I}(V)$. We want to show that either f or g is in $\mathcal{I}(V)$. Consider the decomposition into affine varieties

$$V = \{v \in V : f(v) = 0\} \cup \{v \in V : g(v) = 0\}$$

Since V is irreducible, it follows that either $V = \{v \in V : f(v) = 0\}$ or $V = \{v \in V : g(v) = 0\}$. Hence, either $f \in \mathcal{I}(V)$ or $g \in \mathcal{I}(V)$. □

Proof. (of Corollary 4.36) We first show that $V = \mathcal{V}(I)$ can be written as a union $V = V_1 \cup V_2 \cup \ldots \cup V_r$ of finitely many irreducible affine varieties. We argue by contradiction. Suppose that V is an affine variety that cannot be written in this way. In particular, V is not irreducible. Thus, $V = V_1 \cup V_1'$ with $V_1, V_1' \subsetneq V$ affine varieties. Moreover, V_1 or V_1' is not irreducible. Suppose that V_1 is not irreducible (othwerise change labelling). Thus, $V_1 = V_2 \cup V_2'$ with $V_2, V_2' \subsetneq V_1$ are affine varieties, at least one of which is not irreducible. Suppose that V_2 is not irreducible. Continuing this way, we obtain a chain of affine varieties

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \ldots$$

Applying $\mathcal{I}$ we get a chain of ideals in $k[X_1, \ldots, X_n]$

$$\mathcal{I}(V) \subsetneq \mathcal{I}(V_1) \subsetneq \mathcal{I}(V_2) \subsetneq \mathcal{I}(V_3) \subsetneq \ldots$$

But, this contradicts the fact that $k[X_1, \ldots, X_n]$ is Noetherian. Therefore, $V = V_1 \cup V_2 \cup \ldots \cup V_r$ for some finite r with V_i irreducible affine varieties. Then,

$$\sqrt{I} = \mathcal{I}(V) = \bigcap_{i=1}^{r} \mathcal{I}(V_i)$$

Now, by the previous lemma the ideals $\mathfrak{p}_i = \mathcal{I}(V_i)$ are prime.

Next, observe that $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r$ implies $\sqrt{I} \subset \mathfrak{p}_i$ for all i, hence $\deg HP_{\mathfrak{p}_i}(t) \leq \deg HP_{\sqrt{I}}(t)$. Thus, we have

$$\max\{\deg HP_{\mathfrak{p}_i}(t) | 1 \leq i \leq r\} \leq \deg HP_{\sqrt{I}}(t) = \deg HP_I(t)$$

Let $d := \deg HP_{\sqrt{I}}(t)$ and suppose that $\deg HP_{\mathfrak{p}_i}(t) < d$ for all i. Then, there exist $1 \leq i_1 < i_2 < \ldots < i_d \leq n$ such that $\sqrt{I} \cap k[X_{i_1}, \ldots, X_{i_d}] = \{0\}$ and $f_i \in \mathfrak{p}_i \cap k[X_{i_1}, \ldots, X_{i_d}] \neq \{0\}$ for all i. We have $f = f_1 f_2 \ldots f_r \in \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_2 = \sqrt{I}$. But then, $f \in \sqrt{I} \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$ which is a contradiction. □

The decomposition obtained of $\sqrt{I}$ as an intersection of finitely many primes is unique in the following sense: Call a decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r$ minimal if $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$. Suppose $\sqrt{I} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_\mathfrak{r} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s$ are minimal decompositions into collections of prime ideals $\{\mathfrak{p}_i\}$ and $\{\mathfrak{q}_i\}$ then $r = s$ and the collections coincide up to reordering. Indeed, all we need to observe is the following: Suppose $I \subset \mathfrak{q}$ for a prime ideal $\mathfrak{q}$ then there exists an i such that $\mathfrak{p}_i \subset \mathfrak{q}$. To see this, observe that since $\mathfrak{q}$ is prime, $\sqrt{I} \subset \mathfrak{q}$ hence $\mathcal{V}(\mathfrak{q}) \subset \mathcal{V}(\sqrt{I}) = \mathcal{V}(\mathfrak{p}_1) \cup \mathcal{V}(\mathfrak{p}_2) \cup \ldots \cup \mathcal{V}(\mathfrak{p}_r)$. But, $\mathcal{V}(\mathfrak{q})$ is irreducible (since $\mathfrak{q}$ is prime), hence there exits an i such that $\mathcal{V}(\mathfrak{q}) \subset \mathcal{V}(\mathfrak{p}_i)$ or equivalently, $\mathfrak{p}_i \subset \mathfrak{q}$.

Here is how you can obtain the minimal prime decomposition in Macaulay 2:

```
R = QQ[x,y,z,w,t]
I = ideal(x^2*y-z^3, x*y*w-z^2*t, x*w*t-z*t^2)
J = radical I
C = minprimes J
netList C
```

Let us now summarize the correspondence between algebra and geometry with the following table (we consider $k[X_1, \ldots, X_n]$ with k algebraically closed):

Algebra	Geometry
radical ideal $\sqrt{I}$	affine variety $\mathcal{V}(\sqrt{I})$
$\sqrt{I} + \sqrt{J}$	$\mathcal{V}(\sqrt{I}) \cap \mathcal{V}(\sqrt{J})$
$\sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$	$\mathcal{V}(\sqrt{I}) \cup \mathcal{V}(\sqrt{J})$
$\sqrt{I} : \sqrt{J}$	$\overline{\mathcal{V}(\sqrt{I}) \setminus \mathcal{V}(\sqrt{J})}$
prime ideal $\mathfrak{p}$	irreducible affine variety
maximal ideal $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$	point $(a_1, \ldots, a_n) \in k^n$
prime decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$	irreducible decomposition $\mathcal{V}(\sqrt{I}) = \mathcal{V}(\mathfrak{p}_1) \cup \ldots \cup \mathcal{V}(\mathfrak{p}_r)$

We covered all the items in the table except the 4^{th} row, so let us explain that next.

$\lhd$ Any finite intersection and arbitrary union of affine varieties is an affine variety.

This shows that we can define a topology on k^n in which closed sets are affine varieties. This is called the **Zariski topology**. If $V \subset k^n$ is an affine variety, it can be endowed with the subspace topology: an open set is an intersection with V of an open set in k^n. If $f \in k[X_1, X_2, \ldots, X_n]$ then $U_f = k^n \setminus \mathcal{V}(f)$ is called a **basic open set**.

$\lhd$ Show that the collection of basic open sets U_f for a basis of Zariski topology: Any open set is a union of basic open sets.

$\lhd$ Show that Zariski topology is quasi-compact: Any open cover of k^n has a finite subcover.

Note that when $k = \mathbb{R}$ or $\mathbb{C}$, the Zariski topology is quite different from the usual (Euclidean) topology. Zariski topology is a very weak topology: It has far fewer closed sets. It is not Hausdorff. In fact, any two non-empty open sets intersect.

$\lhd$ Show that if V is an irreducible variety, then any two open sets in the Zariski topology of V intersect.

Proposition 4.39. *The closure in the Zariski topology of $\mathcal{V}(I) \setminus \mathcal{V}(J)$ is contained in $\mathcal{V}(I : J)$, that is,*

$$\overline{\mathcal{V}(I) \setminus \mathcal{V}(J)} \subset \mathcal{V}(I : J)$$

Moreover, equality holds if $I = \sqrt{I}$ is a radical ideal and k is algebraically closed.

◁ Prove Proposition 4.39.

▶ Consider the set of 4 points $S = \{(0,0),(0,1),(1,0),(1,1)\} \subset \mathbb{C}^2$ in the plane. The ideal $I(S) = (X^2 - X, Y^2 - Y)$. To remove two of the points lying on $x = y$, we can consider $I(S) : (x - y)$ and we get $(x + y - 1, y^2 - y)$ and the associated variety is $\{(1,0),(0,1)\}$. Here is how you can do this in Macaulay 2:

```
R= QQ[x,y]
ideal(x^2-x,y^2-y) : ideal (x-y)
```

We have seen that there is an intimate relationship between nilpotent-free k-algebras, that is k-algebras of the form $k[X_1, \ldots, X_n]/\sqrt{I}$, for k algebraically closed, and the affine varieties $\mathcal{V}(\sqrt{I}) \subset k^n$ which are the geometric loci cut out by polynomials. What about maps between such objects?

Definition 4.40. *A* **regular mapping** *between affine varieties $\mathcal{V}(I) \subset k^n$ and $\mathcal{V}(J) \subset k^m$ is a map $\phi : V \to W$ defined by polynomials $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ representing ϕ in the following way*

$$\phi(v_1, v_2, \ldots, v_n) \to (f_1(v_1, \ldots, v_n), f_2(v_1, \ldots, v_n), \ldots, f_m(v_1, v_2, \ldots, v_n))$$

In particular, **regular functions** *on an affine variety $V(I)$ are defined to be the regular mappings $V \to k$ and denoted by $k[V]$.*

By definition, it follows that two polynomial maps $f, g : V \to k$ define the same regular function if and only if $f - g \in \mathcal{I}(V)$. Hence, the algebra of regular functions on V can be identified as

$$k[V] = k[X_1, \ldots, X_n]/\mathcal{I}(V)$$

Now, a k-algebra map (a k-linear ring homomorphism)

$$\phi^* : k[W] = k[Y_1, \ldots, Y_m]/\mathcal{I}(W) \to k[X_1, \ldots, X_n]/\mathcal{I}(V) = k[V]$$

is also determined by m-polynomials $f_1, f_2, \ldots, f_m \in k[X_1, \ldots, X_n]$ by sending

$$Y_i \to f_i(X_1, \ldots, X_n)$$

In fact, by using the Nullstellensatz which gives a bijection between points in $(v_1, \ldots, v_n) \in V$ (resp. $(w_1, \ldots, w_m) \in W$) and the maximal ideals $\mathfrak{m}_{\mathbf{v}} = (X_1 - v_1, X_2 - v_2, \ldots, X_n - v_n) \in k[V]$ (resp. $\mathfrak{n}_{\mathbf{w}} = (Y_1 - w_1, \ldots, Y_m - w_m) \in k[W]$), one can show that $\phi(v_1, v_2, \ldots, v_n) = (w_1, \ldots, w_n)$ if and only if the $\phi^*(\mathfrak{m}_{\mathbf{v}}) = \mathfrak{n}_{\mathbf{w}}$.

We leave it to your algebraic geometry course (or to you as an exercise) to verify the following statement: For k algebraically closed and affine varieties $V \subset k^n$ and $W \subset k^m$, there is a bijection between the k-vector space of regular mappings between $V \to W$ and the k-vector space of algebra homomorphisms $k[W] \to k[V]$. Moreover, this gives an (anti)equivalence between the category of coordinate rings of affine varieties over k and the category of finitely-generated, nilpotent-free algebras over k.

5 Interlude: An application of the Nullstellensatz

We will prove the following theorem.

Theorem 5.1. *(Ax) Suppose $p : \mathbb{C}^n \to \mathbb{C}^n$ is a regular mapping given by $p = (p_1, p_2, \ldots, p_n)$ with $p_i \in \mathbb{C}[X_1, \ldots, X_n]$. If p is injective, then it is also surjective.*

We will need an important consequence of Hilbert's Nullstellensatz that applies to "arithmetic" rings.

Theorem 5.2. *Suppose that A is a finitely generated $\mathbb{Z}$-algebra, i.e. $A \simeq \mathbb{Z}[X_1, \ldots, X_n]/I$. Let $\mathfrak{m} \subset A$ be a maximal ideal, then $A/\mathfrak{m}$ is a finite field.*

Proof. Consider the prime ideal $\mathfrak{m} \cap \mathbb{Z}$ in $\mathbb{Z}$. This can be either (p) for some prime $p \in \mathbb{Z}$ or (0). First, suppose $\mathfrak{m} \cap \mathbb{Z} = (p)$. Then, by $A/\mathfrak{m}$ is a field which is a finitely generated $\mathbb{F}_p = \mathbb{Z}/(p)$ algebra. Thus, by Zariski's lemma (whose proof we saw as part of the proof of the weak Nullstellensatz), we conclude that $A/\mathfrak{m}$ is a finite extension of $\mathbb{F}_p$, hence is finite. Next, consider the case when $\mathfrak{m} \cap \mathbb{Z} = (0)$. Let us write $A = \mathbb{Z}[x_1, \ldots, x_d]$ where $x_i \in A$ are generators of A as a $\mathbb{Z}$-algebra. Now, $A/\mathfrak{m}$ is a field containing $\mathbb{Z}$, hence $\mathbb{Q} \subset A/\mathfrak{m}$. Thus $A/\mathfrak{m}$ is a finitely generated algebra over $\mathbb{Q}$. Now, again by Zariski's lemma, we conclude that $A/\mathfrak{m}$ is a finite extension of $\mathbb{Q}$. So, for each i, there exist polynomial relations with coefficients in $\mathbb{Z}$

$$a_i x_i^{n_i} + \ldots = 0$$

which means $A/\mathfrak{m}$ is an integral extension of the ring $\mathbb{Z}[a_1^{-1}, a_2^{-1}, \ldots, a_d^{-1}] \subset \mathbb{Q}$. But, since $A/\mathfrak{m}$ is a field, this gives that $\mathbb{Z}[a_1^{-1}, \ldots, a_d^{-1}]$ a field by Corollary 4.22, hence it must be that $\mathbb{Z}[a_1^{-1}, \ldots, a_d^{-1}] = \mathbb{Q}$, which contradicts Euclid's result from 300 BC - the infinitude of primes. □

Proof. (of the Theorem of Ax) We first prove the finite field version. Let k be a finite field, if $p : k^n \to k^n$ is injective, then it is obviously surjective (since any injective map between finite fields is surjective).

Next, we use the Nullstellensatz to give algebraic criterion for injectivity and surjectivity.

Injectivity: Let k be a field, and $p_1, p_2, \ldots, p_n \in k[X_1, \ldots, X_n]$ be polynomials such that the regular mapping $p = (p_1, \ldots, p_n) : k^n \to k^n$ is injective. Let $I \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ be the ideal given by

$$I = (p_1(X_1, \ldots, X_n) - p_1(Y_1, \ldots, Y_n), \ldots, p_n(X_1, \ldots, X_n) - p_n(Y_1, \ldots, Y_n))$$

Since p is injective, for all i, we have that $X_i - Y_i \in \mathcal{I}(V(I))$, hence if k is algebraically closed, by Nullstellensatz we can find polynomials $q_{i,j} \in k[X_1, \ldots, X_n, Y_1 \ldots, Y_n]$ for $j = 1, \ldots, n$ and $\ell_i > 0$ such that

$$\sum_{j=1}^{n} (p_j(X_1, \ldots, X_n) - p_j(Y_1, \ldots, Y_n)) q_{i,j}(X_1, \ldots, X_n, Y_1, \ldots, Y_n) = (X_i - Y_i)^{\ell_i}, \ i = 1, \ldots, n \tag{1}$$

Conversely, if Equations (1) is satisfied, over any field k (not necessarily algebraically closed), then $p : k^n \to k^n$ is injective.

Surjectivity: Let $(a_1, \ldots, a_n) \in k^n$ such that the system $p_i(X_1, \ldots, X_n) = a_i$ for $i = 1, \ldots, n$ has no solution. Then, for k algebraically closed, by the Nullstellensatz we must have polynomials $h_i \in k[X_1, \ldots, X_n]$ such that

$$\sum_{i=1}^{n} (p_i(X_1, \ldots, X_n) - a_i) h_i(X_1, \ldots, X_n) = 1 \tag{2}$$

Conversely, if Equation (2) is satisfied, over any field k, then $(a_1, \ldots, a_n) \notin \mathrm{Im}(p)$. Hence, the regular mapping $p : k^n \to k^n$ is not surjective.

Now, we can finally complete the proof of the theorem of Ax for $k = \mathbb{C}$. Suppose that there exists a polynomial mapping $p : \mathbb{C}^n \to \mathbb{C}^n$ given by $p = (p_1, \ldots, p_n)$ that is injective but not surjective. Since $\mathbb{C}$ is algebraically closed, we have polynomials $q_{i,j}$ as in Equations (1) and polynomials h_i as in Equation (2). Let A be a finitely generated $\mathbb{Z}$-algebra that is obtained by adjoining to $\mathbb{Z}$ all the coefficients of the polynomials p_i, $q_{i,j}$, h_i and the a_i, so that the polynomial mapping $p : A^n \to A^n$ makes sense and the Equations (1) and (2) hold in the polynomial ring $A[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ and $A[X_1, \ldots, X_n]$. Finally, let $\mathfrak{m}$ be a maximal ideal in A, and consider the induced mapping

$$\overline{p} : (A/\mathfrak{m})^n \to (A/\mathfrak{m})^n$$

(which is well-defined since $\mathfrak{m} \subset A$ is an ideal). Equations (1) and (2) continue to hold over $A/\mathfrak{m}$ hence $\overline{p}$ is injective but not surjective. But, now by Theorem 5.2, we know that $A/\mathfrak{m}$ is actually a finite field, a contradiction. □

$\lhd$ Show that Nagata's polynomial mapping $p : \mathbb{C}^3 \to \mathbb{C}^3$ given by $(x, y, z) \to (x - 2y(xz + y^2) - z(xz + y^2)^2, y + z(xz + y^2), z)$ is injective (hence also surjective).

$\lhd$ Find a polynomial mapping $p : \mathbb{Q}^n \to \mathbb{Q}^n$ (for any n) which is injective but not surjective.

$\lhd$ Prove that any polynomial mapping $p : \mathbb{R} \to \mathbb{R}$ that is injective is also surjective.

In fact, it is also true that any polynomial mapping $p : \mathbb{R}^n \to \mathbb{R}^n$ that is injective is also surjective. Our proof does not give this more difficult result (which you can read about in a paper by Białynicki-Birula and Rosenlicht titled "Injective morphisms of real algebraic varieties").

6 Abstract commutative algebra

We now begin studying commutative rings via more abstract methods. In particular, we leave the constructive mindset behind for now and admit the consequences of Zorn's lemma. We generally have axiomatics of Noetherian rings in mind but we will not require this at the outset. The first question that we would like to address is that assuming that we are given a general commutative ring A, can we define a space such that A is the algebraic functions on A?

6.1 Spec(A)

Let A be commutative ring with unity. The **maximum spectrum** of a ring is defined to be

$$\mathrm{mSpec}(A) \coloneqq \{\mathfrak{m} \subset A : \mathfrak{m} \text{ is a proper maximal ideal } \}.$$

The constructions $\mathcal{V}$ and $\mathcal{I}$ can then be given as follows: For $I \subset A$ an ideal in A, define

$$\mathcal{V}(I) \coloneqq \{\mathfrak{m} \in \mathrm{mSpec}(A) : I \subset \mathfrak{m}\}$$

and for $S \subset \mathrm{mSpec}(A)$

$$\mathcal{I}(S) \coloneqq \bigcap_{\mathfrak{m} \in S} \mathfrak{m}.$$

If $A = k[X_1, X_2, \ldots, X_n]$ and k is algebraically closed, as we saw before, Hilbert's Nullstellensatz gives that these constructions coincide with the previously geometrically defined ones.

For a more general commutative ring, it turns out using prime ideals is more fruitful. The main problem with the maximal spectrum is that when $f : A \to B$ is a ring homomorphism between rings, it is not true in general that $f^{-1}(\mathfrak{m})$ is not a maximal ideal for $\mathfrak{m}$ a maximal ideal.

We define **spectrum** of the ring A is defined to be

$$\mathrm{Spec}(A) \coloneqq \{\mathfrak{p} \subset A : \mathfrak{p} \text{ is a proper prime ideal } \}$$

The analogues of the constructions $\mathcal{V}$ and $\mathcal{I}$ are as follows: For $I \subset A$ an ideal in A, define

$$\mathscr{V}(I) \coloneqq \{\mathfrak{p} \in \mathrm{Spec}(A) : I \subset \mathfrak{p}\}$$

and for $S \subset \mathrm{Spec}(A)$

$$\mathscr{I}(S) \coloneqq \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$$

We changed the notation from $\mathcal{V}, \mathcal{I}$ to $\mathscr{V}, \mathscr{I}$ since the new constructions do not reproduce the previous ones when $A = k[X_1, X_2, \ldots, X_n]$ (even when k is algebraically closed): $\mathscr{V}(I)$ is in bijection with irreducible affine varieties contained in $\mathcal{V}(I)$.

- If $I_1, \ldots, I_r \subset A$ are ideals, then $\mathscr{V}(I_1 \cap \ldots \cap I_r) = \mathscr{V}(I_1) \cup \ldots \cup \mathscr{V}(I_r)$.
- $\{I_\lambda\}_{\lambda \in \Lambda}$ is a family of ideals in A, then $\mathscr{V}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} \mathscr{V}(I_\lambda)$.
- $\mathscr{V}(\{0\}) = \mathrm{Spec}(A)$ and $\mathscr{V}(A) = \emptyset$.

These properties imply that $\mathrm{Spec}(A)$ is a topological space with closed sets given by $\mathscr{V}(I)$ for I and ideal in A. This is called the (abstract) Zariski topology.

◁ Suppose M is a matrix with entries in $\mathbb{C}$. Consider the $\mathbb{C}$-algebra $\mathbb{C}[M] \coloneqq \{f(M) : f \in \mathbb{C}[X]\}$ where multiplication is given by matrix multiplication. Show that $\mathrm{Spec}(\mathbb{C}[M])$ coincides with the eigenvalues of the matrix M. This is where the name "spectrum" comes from. (Eigenvalues of a Hermitian matrix is known as the spectrum of that Hermitian operator; terminology used in quantum mechanics which can then be traced back to wave spectrum and light.)

$\lhd$ From Proposition 2.5, we see that if $f : A \to B$ is a ring homomorphism we get a map $f^* : \text{Spec}B \to \text{Spec}A$. It is easy to check that this map is continuous in the Zariski topology (check it on basic open sets!).

$\lhd$ Show that the natural map $A \to A/\sqrt{(0)}$ induces a homeomorphism between the prime spectra.

Lemma 6.1. *For $S \subset \text{Spec}(A)$ we have $\mathscr{V}(\mathscr{I}(S)) = \overline{S}$.*

Proof. Clearly $S \subset \mathscr{V}(\mathscr{I}(S))$. Conversely, let $C = \mathscr{V}(I) \subset \text{Spec}(A)$ be a closed set such that $S \subset C$, we need to show that $\mathscr{V}(\mathscr{I}(S)) \subset C$. Since $S \subset C$, we have that for all $\mathfrak{p} \in S$, $I \subset \mathfrak{p}$, then $I \subset \cap_{\mathfrak{p} \in S}\mathfrak{p} = \mathscr{I}(S)$. Hence $C = \mathscr{V}(I) \supset \mathscr{V}(\mathscr{I}(S))$, as required. □

Lemma 6.2. *Let $I \subset A$ be an ideal. Then, $\mathscr{I}(\mathscr{V}(I)) = \sqrt{I}$.*

Proof. This is just the same statement as the one given in Proposition 2.7. □

Note that this is only a formal analogue of the Nullstellensatz that we proved in the case $A = k[X_1, \ldots, X_n]$. It is a much easier result not as deep as the Nullstellensatz. The main difference is that

$$\mathscr{I}(\mathscr{V}(I)) = \bigcap_{I \subset \mathfrak{p}} \mathfrak{p} \text{ and } \mathcal{I}(\mathcal{V}(I)) = \bigcap_{I \subset \mathfrak{m}} \mathfrak{m}.$$

These two expressions coincide for Jacobson rings (by definition) but not in general.

Question: How can A be viewed as functions on Spec$A$?

Let $f \in A$ and $\mathfrak{p} \in \text{Spec}A$, we define the "value" of f at $\mathfrak{p}$ as follows. Since $\mathfrak{p}$ is a prime ideal, $A/\mathfrak{p}$ is an integral domain, so we let $k(\mathfrak{p}) = Frac(A/\mathfrak{p})$ be the fraction field. This field is called the **residue field** at $\mathfrak{p}$. Then, we define $f(\mathfrak{p})$ as the image of f under the composition of the ring homomorphisms:

$$A \to A/\mathfrak{p} \to k(\mathfrak{p})$$

Thus, an element $f \in A$ can be "evaluated" at a point $\mathfrak{p}$ as $f(\mathfrak{p}) \in k(\mathfrak{p})$. Moreover, $f(\mathfrak{p}) = 0$ if and only $(f) \subset \mathfrak{p}$, or equivalently $\mathfrak{p} \in \mathscr{V}((f))$.

Conversely, one can characterize prime ideals in A as the kernel of homomorphisms $A \to k$ where k can be arbitrary field. Thus, we add a point $\mathfrak{p}$ for every possible evaluation homomorphism from A to some field $k(\mathfrak{p})$.

In the geometric case, when $A = k[X_1, \ldots, X_n]/I$ is a finitely generated k-algebra and k is algebraically closed, a maximal ideal is given by $\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ and one can canonically identify $k(\mathfrak{m}) = k[X_1, \ldots, X_n]/\mathfrak{m}$ with k via the homomorphism $A \to k$ that corresponds to the evaluation homomorphism

$$A \to k \quad , \quad f \to f(a_1, a_2, \ldots, a_n)$$

So the above assignment gives back the usual notion of functions on $\mathcal{V}(I)$ under the bijection between maximal ideals in A and the points of $\mathcal{V}(I)$.

In general, the construction views A as a generalized function on $\mathrm{Spec}(A)$ since it possibly takes values in different fields $k(\mathfrak{p})$ depending on the point $\mathfrak{p}$. This is the starting point of Grothendieck's scheme theory. You should take a course on Algebraic Geometry to see how this idea develops further.

▶ Let's consider the case $A = \mathbb{Z}$. Then, $\mathrm{Spec}(\mathbb{Z})$ consist of maximal ideal (p) for prime $p \in \mathbb{Z}$ and the non-maximal, prime ideal (0). An element $n \in \mathbb{Z}$ is viewed as a function which sends

$$(0) \to n \in \mathbb{Q} \quad , \quad (p) \to n \pmod{p} \in \mathbb{F}_p$$

◁ Let A be an integral domain. Prove that $\{(0)\}$ is a dense point in $\mathrm{Spec}(A)$ in the Zariski topology.

◁ Prove that $\mathrm{Spec}\mathbb{Z}$ and $\mathrm{Spec}\overline{\mathbb{Q}}[X]$ are homeomorphic.

Definition 6.3. *Suppose X is a topological space.*

(a) We say that X is Noetherian if all the chains $Y_1 \supset Y_2 \supset \ldots$ with $Y_i \subset X$ closed subspaces stabilise: There exists N such that $Y_N = Y_{N+i}$ for all $i > 0$.

(b) We say that X is reducible if $X = X_1 \cup X_2$ with X_1, X_2 proper closed subspaces of X. Otherwise, we say X is irreducible.

The following statements are proven exactly the same way as in Corollary 4.36 and Lemma 4.38.

▶ Let A be a Noetherian ring, then $X = \mathrm{Spec}A$ is a Noetherian topological space.

▶ Let $Y \subset \mathrm{Spec}(A)$ for a ring A be a closed subset. Then, Y is irreducible if and only if $\mathscr{I}(Y)$ is prime.

▶ If X is a Noetherian topological space, then $X = Y_1 \cup Y_2 \cup \ldots \cup Y_r$ with Y_i closed and irreducible subspaces.

▶ If A is a Noetherian ring and I is a proper ideal. Then there exist a finite number of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ with $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$ such that $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r$. Moreover, if $\mathfrak{q} \in \mathrm{Spec}(A)$ with $I \subset \mathfrak{q}$, then there exists i such that $\mathfrak{p}_i \subset \mathfrak{q}$. In particular, A contains finitely many minimal primes.

6.2 Dimension of a commutative ring

Definition 6.4. *Let X be topological space. We define*

$$\dim X \coloneqq \sup\{n \geq 0 : \exists \;\; X_0 \subsetneq X_1 \subsetneq X_2 \ldots \subsetneq X_n \subset X \text{ with } X_i \text{ closed and irreducible } \}$$

For a ring A, the **Krull dimension** *is defined to be*

$$\dim A \coloneqq \dim \mathrm{Spec}(A) = \sup\{n \geq 0 : \exists \;\; \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \ldots \subsetneq \mathfrak{p}_n \subsetneq A \text{ with } \mathfrak{p}_i \text{ prime } \}$$

For a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, we define its **height** *as*

$$h(\mathfrak{p}) \coloneqq \sup\{n \geq 0 : \exists \;\; \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p} \text{ with } \mathfrak{p}_i \text{ prime } \}$$

▶ Suppose A is an integral domain. $\dim A = 0$ if and only if A is a field.

▶ Let $A = k[X_1, \ldots, X_n]$ then we have a chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, X_2, \ldots, X_n) \subsetneq A$. Hence $\dim A \geq n$. We will see later that in fact $\dim A = n$.

▶ Suppose A is a UFD and $\mathfrak{p} \subset A$ is a prime ideal. $h(\mathfrak{p}) = 1$ if and only if $\mathfrak{p} = (a)$ with $a \in A$ an irreducible element. In particular, $\dim \mathbb{Z} = 1$ and $\dim k[X] = 1$.

You can also use Macaulay 2 to compute Krull dimension of a ring as follows:

```
R = QQ[X,Y,Z]
dim R
R = QQ[X,Y]/(X^2,Y^3,X*Y^2)
dim R
R = ZZ[X]
dim R
```

We next want to understand rings which have $\dim A = 0$ that are not fields. It turns out there is a nice characterisation of such rings in terms of chain conditions on their ideals.

Definition 6.5. *Let A be a ring M be an A-module.*

(a) We say that M is **Noetherian** *if of all the ascending chains of A-submodules*

$$M_1 \subset M_2 \subset \ldots \subset M$$

become stationary.

(b) We say that M is **Artinian** *if all of the descending chains of A-submodules*

$$M \supset M_1 \supset M_2 \supset \ldots$$

become stationary.

(c) A ring A is Noetherian or Artinian if A as an A-module is Noetherian or Artinian.

◁ Suppose A is Noetherian and M is a finitely generated A-module. Then M is Noetherian.

Note that A-submodules of A as an A-module are just ideals in A. So, the notion of Noetherian ring A is the same as what we saw before in terms of ideals in A.

The condition of being an Artinian ring is also important. Despite the similarity in definition, being an Artinian ring is much more restrictive. Here is a first indication of this.

Proposition 6.6. *In an Artinian ring every prime ideal is maximal.*

Proof. Let A be an Artinian ring and $\mathfrak{p} \subset A$ is a prime ideal. $A/\mathfrak{p}$ is also Artinian and an integral domain. We want to show that it is in fact a field. Thus, we want to show that any $a \in A/\mathfrak{p}$ is invertible. Consider the descending sequence of ideals

$$(a) \supset (a^2) \supset \ldots$$

This has to stabilise. Hence $(a^n) = (a^{n+1})$ for some $n > 0$. This implies $a^n = ba^{n+1}$ for some b, or $a^n(1 - ba) = 0$. Since $a^n \neq 0$ and $A/\mathfrak{p}$ is an integral domain, we deduce that $(1 - ba) = 0$. □

We can now state the characterisation of 0-dimensional Noetherian rings.

Theorem 6.7. *Let A be a Noetherian ring. Then $\dim A = 0$ if and only if A is also Artinian.*

Proof. We have seen that every prime ideal in an Artinian ring is maximal, so that implies $\dim A = 0$.

To prove the converse statement, that is, the statement that $\dim A = 0$ implies A is Artinian, we will develop a few preliminary results.

Definition 6.8. *We say than an A-module M is* **simple** *if $\{0\}$ and M are the only A-submodules of M.*

▶ If $\mathfrak{m} \subset A$ is a maximal ideal. Then $A/\mathfrak{m}$ is a field, hence cannot have a non-trivial submodule. Therefore, $A/\mathfrak{m}$ is a simple module. Conversely, a simple module M is necessarily of the form $A/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$. Indeed, if $v \in M$ is any non-zero element, we have $A \cdot v \subset M$ is a submodule. Hence, $A \cdot v = M$. Thus, A is cyclic module and$M$ is isomorphic to A/I where $I = \text{ann}M$. Now, let m be a maximal ideal containing I, then $\mathfrak{m}/I$ is a submodule of $M = A/I$, hence it must be the case that $\mathrm{m} = I$.

A chain of A-submodules $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_n = \{0\}$ is called a **Jordan-Hölder series** or **composition series** if each module M_i/M_{i+1} is a simple A-module. In this case n is called the **length** of M and is denoted $\ell(M)$. The exercise below shows that $\ell(M)$ is well-defined.

Proposition 6.9. *(Jordan-Hölder decomposition) M admits a Jordan-Hölder series if and only if M is Noetherian and Artinian.*

Clearly, it is necessary that every ascending chain and descending chain stabilises since otherwise we cannot get a finite chain. The proof of the other direction is also easy since you can just keep adding submodules to a chain until you ensure that the quotient modules are simple.

◁ Prove that every composition series of M is unique in the following sense: If $M = M_0 \supsetneq M_1 \supsetneq \ldots \supsetneq M_p = \{0\}$ and $M = N_0 \supsetneq N_1 \supsetneq \ldots \supsetneq N_q = \{0\}$ are two composition series of M. Then, $p = q$ and there exists a one-to-one correspondence between the set of quotients $(M_{i-1}/M_i)_{1 \leq i \leq p}$ and $(N_{i-1}/N_i)_{1 \leq i \leq q}$. The proof is the same as in the case of finite groups, so we leave this as an exercise. In particular $\ell(M)$ is well-defined.

We are now ready to prove that a Noetherian algebra with $\dim A = 0$ is Artinian. Since $\dim A = 0$ all the prime ideals are maximal, and since A is Noetherian, there exist finitely many of these, call them $\mathfrak{m}_i$ such that $I = \sqrt{(0)} = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_r$ and $\mathfrak{m}_i \not\subset \mathfrak{m}_j$ if $i \neq j$. We have $\mathfrak{m}_i + \mathfrak{m}_j = A$ for $i \neq j$. In other words, $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r$ are pairwise coprime. By the Sunzi remainder theorem 2.3, we have that

$$\mathfrak{m}_1 \mathfrak{m}_2 \ldots \mathfrak{m}_r = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_r = I$$

Consider the chain of ideals

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \ldots \supset I = \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_r \supset I\mathfrak{m}_1 \supset I\mathfrak{m}_1\mathfrak{m}_2 \ldots \supset I^2 \supset \ldots \supset I^3 \supset \ldots \supset I^{Nn} = \{0\}$$

Here $I = \sqrt{(0)} = (a_1, \ldots, a_n)$ for some generators by the Noetherian property. Moreover, there exists N such that $a_i^N = 0$e for all i, hence it follows that $a^{Nn} = 0$ for all $a \in I$.

Now, let us consider the consecutive terms in this chain. Any such term is of the for $M \supset M\mathfrak{m}_i$ for some i and M an ideal of A. Thus, the A-module structure on $M/M\mathfrak{m}_i$ reduces to the structure of a finite-dimensional (since A is Noetherian) vector space over the field $A/\mathfrak{m}_i$. Thus, we can find a chain of subspaces with 1-dimensional subquotients. As a result, $M/M\mathfrak{m}_i$ admits a composition series as an A-module. Therefore, A admits a composition series. By the Jordan-Hölder theorem, it follows that A is Artinian. □

A local Artinian ring is called a **primary ring**. These are precisely the rings R which contain at most one prime ideal.

▶ $\mathbb{Z}/(p^s)$ and $k[x]/(x^s)$ are primary rings.

Theorem 6.10. *Every Artinian ring is a product of primary rings (in a unique way).*

Proof. We saw in the proof of the previous result that in an Artinian ring there are finitely many distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ with $\sqrt{(0)} = \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_r$. We also saw that there exists s such that $\sqrt{(0)}^s = (0)$. Hence, we have

$$(0) = \mathfrak{m}_1^s\mathfrak{m}_2^s \ldots \mathfrak{m}_r^s = \mathfrak{m}_1^s \cap \mathfrak{m}_2^s \cap \ldots \cap \mathfrak{m}_t^s$$

(Note that since $\mathfrak{m}_i$ and $\mathfrak{m}_j$ are coprime for $i \neq j$, we also have $\mathfrak{m}_i^s$ and $\mathfrak{m}_j^s$ are coprime.) So, we can now apply the Sunzi remainder theorem to get

$$R = R/(0) = R/\mathfrak{m}_1^s \times R/\mathfrak{m}_2^s \times \ldots \times R/\mathfrak{m}_r^s$$

We leave the uniqueness statement as an exercise. □

6.3 Localisation

We next discuss an important construction in algebra that is the algebraic analogue of geometric notion of concentrating attention near a point.

Let A be an integral domain an S is a subset of A not containing 0, we can then consider the subring

$$S^{-1}A = A[\{1/s | s \in S\}] \subset FracA$$

There is the inclusion homomorphism $A \to S^{-1}A$ and every element of S becomes invertible in $S^{-1}A$. Recall that in the construction of $FracA$ we use an equivalence relation which declares $\frac{a}{s} = \frac{b}{s'}$ if $as' - bs = 0$. More generally, if A is not an integral domain but S does not contain any zero divisors, then same construction works.

Now, given a ring A and S be multiplicatively closed set (with $1 \in S$) which possibly includes zero divisors, we would like to construct a ring B and a homomorphism $\iota : A \to B$ such that $\iota(s)$ is invertible for all S. The idea is very simple: We want to embed A in a bigger ring B such that the elements of S become invertible, but if there exists $a \in A$ and $s \in S$ such that $as = 0$,

then invertibility of S would imply $a = 0$, hence we have to quotient out by such a first and then we can carry out the construction from before. It turns out this can be done in a fairly straightforward way directly by imitating the construction of the field of fractions of an integral domain with only a small modification in the definition of the equivalence relation to allow for zero divisors.

Definition 6.11. *Consider the set $A \times S$ with the equivalence relation*

$$(a, s) \sim (b, s') \text{ if and only if there exists } t \in S \text{ such that } t(as' - bs) = 0$$

Writing $\frac{a}{s}$ for the equivalence class of (a, s), we define the **ring of fractions** $S^{-1}A \coloneqq \{\frac{a}{s} | a \in A, s \in S\}$ *with the following rules for addition and multiplication:*

$$\frac{a}{s} + \frac{b}{s'} \coloneqq \frac{as' + bs}{ss'}$$

$$\frac{a}{s} \cdot \frac{b}{s'} \coloneqq \frac{ab}{ss'}$$

$S^{-1}A$ is also called the **localisation** of A with respect to S.

◁ We leave it as an exercise the verification that this construction defines a ring $S^{-1}A$. The verification of the transitivity of the equivalence relation is instructive in explaining the definition.

▶ There is a homomorphism $\iota : A \to S^{-1}A$ given by $a \to \frac{a}{1}$ and it satisfies $\iota(s)\frac{1}{s} = 1$ for all $s \in S$. One often omits ι from the notation and writes $a \in S^{-1}A$ instead of $\iota(a) \in S^{-1}A$ for $a \in A$. Similarly, if $I \subset A$ is an ideal, we write $S^{-1}I \coloneqq IS^{-1}A$ for the ideal $\iota(I)S^{-1}A$ of $S^{-1}A$. The kernel of ι is given by $\ker(\iota) = \{a \in A : \frac{a}{1} = \frac{0}{1}\} = \{a \in A : \exists t \in S,\ at = 0\}$. In particular, ι is injective if A is an integral domain.

▶ Localisation satisfies the following universal property: Suppose B is a ring and $g : A \to B$ is a ring homomorphism such that $g(s)$ is invertible for all S. Then there exists a unique homomorphism $h : S^{-1}A \to B$ such that $g = h \circ \iota$. Indeed, one defines $h(a/s) = g(a)g(s)^{-1}$ and verifies that this is a well-defined homomorphism of rings and is the unique such that does the job.

◁ Given a ring A and a multiplicative set S. Let $\mathfrak{n} = \{a \in A : \exists t \in S,\ at = 0\}$ be the ideal of zero divisors with respect to S. Let $\overline{S}$ be the multiplicative set given as the image of S in $A/\mathfrak{n}$. Observe that $\overline{S}$ in $A/\mathfrak{n}$ does not contain any zero divisors. Show that $\overline{S}^{-1}(A/\mathfrak{n})$ is isomorphic to $S^{-1}A$.

The following two are the main examples of localisation:

(a) Let $f \in A$ and $S \coloneqq \{f^n : n = 1, 2, \ldots\} \cup \{1\}$ multiplicatively closed set. Then we write $A_f \coloneqq S^{-1}A$. We have $\ker(\iota) = \{a \in A : \exists n \geq 0,\ af^n = 0\}$. We see that $A_f = \{0\}$ if and only if f is nilpotent.

◁ Prove that A_f is isomorphic to the ring $A[X]/(Xf - 1)$.

◁ Consider the ring $k[X,Y]/XY$ and let $S = \{1, X, X^2, \ldots\}$. Show that $S^{-1}A = A_X$ is isomorphic to the ring $k[X, X^{-1}]$.

▶ Consider the ring $\mathbb{Z}$ and $0 \neq b \in \mathbb{Z}$, then $\mathbb{Z}_b = \{\frac{a}{b^s} \in \mathbb{Q} : s \in \mathbb{Z}_{\geq 0}\}$.

(b) Let $\mathfrak{p}$ be a prime ideal and $S \coloneqq A \setminus \mathfrak{p}$ multiplicatively closed set. We note $A_\mathfrak{p} \coloneqq S^{-1}A$ which is a local ring with the unique maximal ideal given by $\mathfrak{m} = S^{-1}\mathfrak{p}$ (see Lemma 6.12).

▶ Suppose A is an integral domain then $\mathfrak{p} = (0)$ is a prime ideal, and $A_{(0)}$ is the field of fractions of A.

▶ Consider the prime ideal $(p) \subset \mathbb{Z}$, then $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$

▶ Consider the maximal ideal (X) in $k[X]$, then $k[X]_{(X)} = \{\frac{f}{g} \in k(X) : X \nmid g\}$.

Here are some basic properties of localisation.

Lemma 6.12. *(i) Let $J \subset S^{-1}A$ be an ideal and $I = \iota^{-1}(J) \subset A$. Then $J = S^{-1}I$. In particular, this implies that $S^{-1}(A)$ is Noetherian if A is Noetherian.*

(ii) The canonical map $\iota^{-1} : \mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ sending is an order preserving bijection onto the subset $\{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$ with inverse given by $\mathfrak{p} \to S^{-1}\mathfrak{p}$ for $\mathfrak{p} \cap S = \emptyset$.

(iii) (Localisation commutes with quotients) Let I be an ideal in A. Write $\overline{S}$ for the image of S under the canonical ring homomorphism $A \to A/I$. Then, $\overline{S}^{-1}(A/I) \simeq S^{-1}A/S^{-1}I$.

Proof. (i))It is clear that $S^{-1}I \subset J$. Conversely, suppose $x = a/s \in J$. Then $s.x = \frac{s}{1}\frac{a}{s} = \frac{a}{1} \in J$ hence, $a \in \iota^{-1}J = I$.

(ii) Let $\mathfrak{q} \subset S^{-1}A$ be a prime ideal and let $\mathfrak{p} = \iota^{-1}(\mathfrak{q})$ be the prime ideal in A. From, part (i), we have $\mathfrak{q} = S^{-1}\mathfrak{p}$. We have that $\mathfrak{p} \cap S = \emptyset$ otherwise, $\mathfrak{q}$ would contain a unit of $S^{-1}A$. Conversely, let $\mathfrak{p} \subset A$ be a prime ideal, then $S^{-1}\mathfrak{p} \subset S^{-1}A$ is a prime ideal. Indeed, if $\frac{a}{s}\frac{b}{t} = \frac{p}{r} \in S^{-1}\mathfrak{p}$, $a, b \in A$, $p \in \mathfrak{p}$, $s, t, r \in S$ then there exists $u \in S$ such that $u(abr - pst) = 0$. So, we have $abru = pust \in \mathfrak{p}$ but $ru \in S$ and $\mathfrak{p} \cap S = \emptyset$. Hence, $ab \in \mathfrak{p}$. Thus, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. It follows that either $a/s \in S^{-1}\mathfrak{p}$ or $b/t \in S^{-1}\mathfrak{p}$. Furthermore, we have $S^{-1}\mathfrak{p} \neq S^{-1}A$. Suppose that $1 = \frac{p}{s}$ with $p \in \mathfrak{p}$ and $s \in S$, then there exits $t \in S$ such that $t(s - p) = 0$. Hence, $ts = tp \in S \cap \mathfrak{p} = \emptyset$ which is a contradiction. From part (i), we see that $S^{-1}(\iota^{-1}\mathfrak{q}) = \mathfrak{q}$ which shows that ι^{-1} is injective. Finally, we have to show that it is surjective onto $\{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$. We will show that $\mathfrak{p} = \iota^{-1}S^{-1}\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\mathfrak{p} \cap S = \emptyset$. It is clear that $\mathfrak{p} \subset \iota^{-1}S^{-1}(\mathfrak{p})$. To see the reverse inclusion, consider an element $a \in \iota^{-1}S^{-1}(\mathfrak{p})$. Then $\frac{a}{1} = \frac{p}{s} \in S^{-1}(\mathfrak{p})$ for some $p \in \mathfrak{p}$ and $s \in S$. Thus, there exits a $t \in S$ such that $tsa = tp \in \mathfrak{p}$. It follows that $a \in \mathfrak{p}$ since $s, t \in S$ and $\mathfrak{p} \cap S = \emptyset$.

(iii) Both sides have the universal property for ring homomorphisms $g : A \to C$ such that g maps elements of S to units of C and g maps elements of I to 0. The isomorphism follows from the uniqueness of the solution to this universal mapping problem. More concretely, one can construct an explicit map sending $a/s + S^{-1}I \in S^{-1}A/S^{-1}I$ to $\frac{a+I}{s+I} \in \overline{S}^{-1}(A/I)$. It is easy to check directly that this is a ring homomorphism that induces an isomorphism. □

The particular case of Lemma 6.12 applied to $S = \{f^n : n = 1, 2, \ldots\} \cup \{1\}$ for fixed $f \in A$ gives the following:

Corollary 6.13. *For $f \in A$, define basic open sets $D(f) = \{\mathfrak{p} \in \mathrm{Spec}A : f \notin \mathfrak{p}\} = \mathrm{Spec}A \backslash \mathscr{V}(f)$. Then $\mathrm{Spec}A_f = D(f)$.*

Thus, the localisation A_f is giving us "regular functions" on the principal open set $D(f)$.

The particular case of Lemma 6.12 applied to $S = A \backslash \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Spec}(A)$ gives the following:

Corollary 6.14. *If $\mathfrak{p} \subset A$ is a prime ideal and $S = A \setminus \mathfrak{p}$. Then $A_\mathfrak{p} \coloneqq S^{-1}A$ is a local ring with the unique maximal ideal $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p}$. Moreover, there is a bijection $\mathrm{Spec}(A_\mathfrak{p})$ to $\{\mathfrak{q} \in \mathrm{Spec}(A) : \mathfrak{q} \subset \mathfrak{p}\}$. In particular, $\dim A_\mathfrak{p} = h(\mathfrak{p})$ in A.*

▶ The passage from A to $A_\mathfrak{p}$ cuts out all the prime ideals except those contained in $\mathfrak{p}$. This is in contrast to the passage from A to $A/\mathfrak{p}$ which cuts out all the prime ideals except those containing $\mathfrak{p}$. Given primes ideals $\mathfrak{q} \subset \mathfrak{p}$, we can also localise with respect to $\mathfrak{p}$ and quotient with respect to $\mathfrak{q}$ to restrict our attention to prime ideals which lie between $\mathfrak{p}$ and $\mathfrak{q}$.

◁ Let I be an ideal in A, show that $\iota^{-1}S^{-1}I = \{a \in A : as \in I \text{ for some } s \in S\}$.

Localisation gives a way of concentrate our attention to near a point $\mathfrak{p} \in$ SpecA by considering the ring $A_\mathfrak{p}$ which is the algebraic analog of germs of functions defined near $\mathfrak{p}$. In particular, $\dim A$ can be computed as the supremum of dimensions $\dim A_\mathfrak{p}$.

6.4 Dimension for local rings

Next, we come to a very useful lemma in the study of local rings, which will later on help us understand how to compute $\dim A_\mathfrak{p}$.

Lemma 6.15. *(Nakayama's Lemma) Let A be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated A-module and $N \subset M$ be a submodule with the property that $M = N + \mathfrak{m}M$. Then, $M = N$.*

This is a simple but important result that allows us to make deductions about properties of M as an A-module from the properties of $M/\mathfrak{m}\mathfrak{M}$ as an $A/\mathfrak{m}$-vector space. Thus, many properties of the finite-dimensional modules over a local ring A can be studied via linear algebra over the field $A/\mathfrak{m}$.

Proof. Let $\overline{M} = M/N$ be the finitely generated A-module with $\overline{M} = \mathfrak{m}\overline{M}$. We want to show that $\overline{M} = 0$. Suppose $x_1, \ldots, x_n \in \overline{M}$ be such that $\overline{M} = Ax_1 + Ax_2 + \ldots + Ax_n$ with $n \geq 1$ minimal. Since $\overline{M} = \mathfrak{m}\overline{M}$, we have $x_n = \sum_{i=1}^n a_i x_i$ with $a_i \in \mathfrak{m}$. Then, $(1 - a_n)x_n = \sum_{i=1}^{n-1} a_i x_i$ but $(1 - a_n) \in A \setminus \mathfrak{m}$ is invertible. It follows that $x_n \in Ax_1 + Ax_2 + \ldots + Ax_{n-1}$, contradicting the minimality of n. □

Here is first application of Nakayama's lemma:

Proposition 6.16. *Let A be a local ring with maximal ideal $\mathfrak{m}$, let $k = A/\mathfrak{m}$ be the residue field. Let M be a finitely generated A-module. Define*

$$\mu(M) \coloneqq \min\{\exists\ x_1, \ldots, x_n \in M : M = Ax_1 + Ax_2 + \ldots + Ax_n\}$$

Then $\dim_k M/\mathfrak{m}M = \mu(M)$.

Proof. Suppose $M = Ax_1 + Ax_2 + \ldots + Ax_n$. Denote $\overline{x} \in M/\mathfrak{m}M$ the image of an element $x \in M$ in the quotient. Then $M/\mathfrak{m}M = \langle \overline{x}_1, \ldots, \overline{x}_n \rangle_k$. Hence, $\dim_k M/\mathfrak{m}M \leq n$. Conversely, suppose $x_1, x_2, \ldots, x_n \in M$ such that $\overline{x}_1, \ldots, \overline{x}_n$ is a basis as a k-vector space of $M/\mathfrak{m}M$. We want to show that $Ax_1 + Ax_2 + \ldots + Ax_n = M$. Let $N = Ax_1 + Ax_2 + \ldots + Ax_n \subset M$. By Nakayama's lemma, it suffices to show that $M = N + \mathfrak{m}M$. The fact that $N + \mathfrak{m}M \subset M$ is clear. To show inclusion in the other direction, let $x \in M$. Then, $\overline{x} = \sum_{i=1}^n \overline{a}_i \overline{x}_i$ where $\overline{a}_i \in k = A/\mathfrak{m}$ are the images of some elements $a_i \in A$. Thus, $x - \sum_{i=1}^n a_i x_i \in \mathfrak{m}M$, and so $x \in \mathfrak{m}M + N$ since $\sum_{i=1}^n a_i x_i \in N$. □

As a special case, consider A a local Noetherian ring with maximal ideal $\mathfrak{m}$ and $M = \mathfrak{m}$ - a finitely generated A-module. We define $\mu(A) \coloneqq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Question: What is the relation between $\mu(A)$ and $\dim A$?

The answer will be given by the following important theorem of Krull which provide a lower estimate of the number of generators of an ideal in a Noetherian ring (and the number of equations needed to describe an affine variety).

Theorem 6.17. *(Krull) Let A be a Noetherian ring. $I = (a_1, \ldots, a_r)$ be an ideal generated by r elements. Let $\mathfrak{p} \subset A$ be a prime ideal which is minimal (with respect to inclusion) among prime ideals such that $I \subset \mathfrak{p}$. Then,*

$$h(\mathfrak{p}) \leq r$$

As an example, suppose A is a Noetherian local ring with maximal ideal $\mathfrak{m}$, and $k = A/\mathfrak{m}$. We have

$$\mu(A) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = \min\{r \geq 0 : \mathfrak{m} = (a_1, \ldots, a_r)\} < \infty$$

Then Krull's theorem (applied to $I = \mathfrak{m}$) gives

$$\dim(A) = h(\mathfrak{p}) \leq \mu(A)$$

This inequality provides the intuition that adding one equation can decrease the dimension of the space of solutions by at most one. Note that one can give a lower bound for $\dim A$ by exhibiting a chain of prime idels in A, however giving an upper bound from the definition is not straightforward. This is another reason why Theorem 6.17 is important.

Definition 6.18. *A local Noetherian ring A is said to be* **regular** *if* $\dim(A) = \mu(A)$.

An important characterisation theorem due Auslander-Buchsbaum states that regular local rings are UFDs. Unfortunately, we don't have time to prove this result in this course (see [4]).

▶ The local ring $k[X_1, \ldots, X_n]_{\mathfrak{p}}$, the localisation of $k[X_1, \ldots, X_n]$ at a prime ideal $\mathfrak{p}$ is regular.

The general case of Krull's theorem is obtained by induction on n; the case $n = 1$ is then the hardest part of the proof which we state separately before giving a proof.

Theorem 6.19. *(Krull's principal ideal theorem) Let A be a Noetherian ring and $a \in A$ be a non-unit. Let $I = (a)$. Let $\mathfrak{p}$ be a prime ideal minimal among prime ideals such that $a \in \mathfrak{p}$. Then $h(\mathfrak{p}) \leq 1$.*

Proof. Let us first explain why we may suppose A is a local ring with maximal ideal $\mathfrak{p}$. Indeed, consider the localisation $A_{\mathfrak{p}}$. Then the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ is the minimal prime ideal containing $\frac{a}{1} \in A_{\mathfrak{p}}$ and also $h(\mathfrak{p}) = \dim A_{\mathfrak{p}} = h(\mathfrak{p}A_{\mathfrak{p}})$ by Corollary 6.14.

Therefore, we may suppose that A is a local ring with maximal ideal $\mathfrak{p}$. We want to show that $\dim A = h(\mathfrak{p}) \leq 1$. Equivalently, for all $\mathfrak{q} \subsetneq \mathfrak{p}$, we want to show that $h(\mathfrak{q}) = 0$. Consider the localisation $\iota : A \to A_{\mathfrak{q}}$. This is a local ring with maximal ideal $S^{-1}(\mathfrak{q})$. Our goal is to show that $S^{-1}(\mathfrak{q})$ is nilpotent, that is $S^{-1}(\mathfrak{q}) \subset \sqrt{(0)}$ in $A_{\mathfrak{q}}$. For then, since $\sqrt{(0)}$ is the intersection of all prime ideals in $A_{\mathfrak{q}}$, it follows that $S^{-1}(\mathfrak{q})$ is the unique maximal ideal in $A_{\mathfrak{q}}$. Hence, $h(\mathfrak{q}) = \dim A_{\mathfrak{q}} = 0$, as required.

To see that $S^{-1}(\mathfrak{q})$ is nilpotent, let's consider the chain of ideals in $A_{\mathfrak{q}}$ given by powers of $S^{-1}(\mathfrak{q})$:

$$S^{-1}(\mathfrak{q}) \supset S^{-1}(\mathfrak{q}^2) \supset \ldots$$

We let $\mathfrak{q}^{(n)} = \iota^{-1}S^{-1}(\mathfrak{q}^n)$ be the **$\mathbf{n^{th}}$ symbolic power** of $\mathfrak{q}$. Explicitly,

$$\mathfrak{q}^{(n)} = \{a \in A : as \in \mathfrak{q}^n \text{ for some } s \in A \setminus \mathfrak{q}\}$$

These give a chain of ideals in A

$$\mathfrak{q} = \mathfrak{q}^{(1)} \supset \mathfrak{q}^{(2)} \supset \ldots$$

We claim that this chain stabilizes. Let us consider the chain of ideals

$$\mathfrak{p} \supset (a) + \mathfrak{q}^{(1)} \supset (a) + \mathfrak{q}^{(2)} \ldots$$

Passing to the quotient $\overline{A} = A/(a)$, we get a chain

$$\overline{\mathfrak{p}} \supset \overline{\mathfrak{q}}^{(1)} \supset \overline{\mathfrak{q}}^{(2)} \ldots$$

of ideals in $\overline{A}$. Because $\mathfrak{p}$ is minimal, $\overline{\mathfrak{p}} = \mathfrak{p}/(a)$ is the only prime ideal in $A/(a)$. Hence, $\dim A/(a) = 0$. Therefore, by Theorem 6.7, $A/(a)$ is Artinian. Therefore, there exists n such that $\overline{\mathfrak{q}}^{(n)} = \overline{\mathfrak{q}}^{(n+1)}$. Hence, we have

$$(a) + \mathfrak{q}^{(n)} = (a) + \mathfrak{q}^{(n+1)}.$$

It follows that for $x \in \mathfrak{q}^{(n)}$, we can find $r \in A$ and $y \in \mathfrak{q}^{(n+1)}$ such that $x = ra + y$. But then $ra = x - y \in \mathfrak{q}^{(n)}$. Hence $\iota(r)\iota(a) = \iota(ra) \in S^{-1}(\mathfrak{q}^n)$. But, since $a \notin \mathfrak{q}$, $\iota(a)$ is invertible in $A_\mathfrak{q}$ hence, $\iota(r) \in S^{-1}(\mathfrak{q}^n)$. Therefore, $r \in \mathfrak{q}^{(n)}$. It follows that

$$\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$$

and since $a \in \mathfrak{p}$, we also have $\mathfrak{q}^{(n)} = \mathfrak{p}\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. Now, consider $\mathfrak{q}^{(n)}$ as an A-module and $\mathfrak{q}^{(n+1)}$ as a submodule. Applying Nakayama's lemma, we conclude that

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}.$$

Hence, $S^{-1}(\mathfrak{q}^n) = S^{-1}(\mathfrak{q}^{n+1}) = S^{-1}(\mathfrak{q})S^{-1}(\mathfrak{q}^n)$. Applying Nakayama's lemma once again, this time for the $A_\mathfrak{q}$-module $S^{-1}(\mathfrak{q}^n)$, we conclude that $S^{-1}(\mathfrak{q}^n) = 0$. We conclude that $A_\mathfrak{q}$ is a local ring whose maximal ideal $S^{-1}(\mathfrak{q})$ is nilpotent, hence is of dimension zero. □

◁ Carefully examine the proof to see why we needed to use the symbolic powers $\mathfrak{q}^{(n)}$ rather than the ordinary n^{th} powers $\mathfrak{q}^n$ of the ideal $\mathfrak{q}$.

◁ Supppose A is Noetherian, and $\sqrt{(0)} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$ is the minimal prime decomposition of the nilradical. Show that $\cup_{i=1}^s \mathfrak{p}_i$ consists of zero divisors alone. Use this to show that, with the assumptions of Theorem 6.19, one has $h(\mathfrak{p}) = 1$ if a is a zero-divisor.

◁ Show that for $\mathfrak{p} = (x^4 - yz, y^2 - xz, x^3y - z^2) \subset k[x, y, z]$, $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$.

Proof. (of Theorem 6.17) We proved the case of $r = 1$, and we now want to deduce the general case by induction. Again by localizing we may suppose that A is local and $\mathfrak{p}$ is the maximal ideal with property that it is the minimal prime ideal containing $I = (a_1, \ldots, a_r)$.

We choose a prime ideal $\mathfrak{p}_1 \subsetneq \mathfrak{p}$ and maximal with this property, or equivalently $h(\mathfrak{p}_1) = h(\mathfrak{p}) - 1$. We want to find an ideal I_1 generated by $(r-1)$ elements contained in $\mathfrak{p}_1$ with the property that $\mathfrak{p}_1$ is the minimal prime ideal containing I_1. Then by induction, we get $h(\mathfrak{p}_1) \leq (r-1)$ and so the theorem follows.

By assumption (of minimality of $\mathfrak{p}$), $\mathfrak{p}_1$ cannot contain all the a_i's. For definiteness, suppose $a_1 \notin \mathfrak{p}_1$. Now, let $J = (a_1) + \mathfrak{p}_1$. We have that $\mathfrak{p} \supset J$ and is the minimal prime ideal with this property.

We have $\sqrt{J} = \mathfrak{p}$. To see this, note that since A is Noetherian, we can write $\sqrt{J} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$ such that $J \subset \mathfrak{q}_i \subset \mathfrak{p}$. But, since $\mathfrak{p}$ is minimal prime ideal containing J, it follows that $\mathfrak{q}_i = \mathfrak{p}$ for all i.

Therefore, there exists N, such that $a_i^N \in J$ for all i. Hence, for all $i = 2, \ldots, r$ there exists $x_i \in A$ and $y_i \in \mathfrak{p}_1$ such that

$$a_i^N = a_1 x_i + y_i$$

We define $I_1 \coloneqq (y_2, \ldots, y_r)$. We claim that $\mathfrak{p}_1$ is minimal among prime ideals containing I_1. Indeed, consider the quotient map $\pi : A \to A/I_1$. Write $\pi(a) = \overline{a}$. We have $(0) \neq (\overline{a}_1) \subset \overline{\mathfrak{p}} \subset$

A/I_1. We claim that $\overline{\mathfrak{p}}$ is minimal in A/I_1 with $(\overline{a}_1) \subset \overline{\mathfrak{p}}$. It suffices to show that $\sqrt{(\overline{a}_1)} = \overline{\mathfrak{p}}$. To see this, first observe that

$$(a_1, y_2, \ldots, y_r) = (a_1, a_2^N - a_1x_2, a_3^N - a_1x_3, \ldots, a_r^N - a_1x_r) = (a_1, a_2^N, a_3^N, \ldots, a_r^N)$$

On the other hand, we have $I = (a_1, \ldots, a_r) \subset \mathfrak{p}$ and $\mathfrak{p}$ is minimal with this property, so as before $\sqrt{I} = \mathfrak{p}$. This means that for any $x \in \mathfrak{p}$ there is some power $x^s \in I$, hence, $x^{srN} \in (a_1^N, a_2^N, \ldots, a_r^N) \subset (a_1, y_2, \ldots, y_r)$. It follows that $\sqrt{(a_1, y_2, \ldots, y_r)} = \mathfrak{p}$. This, in turn, implies that $\sqrt{(\overline{a}_1)} = \overline{\mathfrak{p}}$. Finally, by the Hauptidealsatz, we have $h(\overline{\mathfrak{p}}) \leq 1$. Hence $h(\overline{p}_1) = 0$ which in turn implies that $\mathfrak{p}_1$ is minimal prime ideal containing I_1, as required. □

Corollary 6.20. *Let k be an algebraically closed field,* $\dim k[X_1, X_2, \ldots, X_n] = n$.

Proof. Let $A = k[X_1, X_2, \ldots, X_n]$. We have already seen that $\dim A \geq n$ because of the existence of the chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n) \subsetneq A$. Let $(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \ldots \subsetneq \mathfrak{p}_r \subsetneq A$ be a chain of prime ideal with $\mathfrak{p}_r$ a maximal ideal. By Hilbert's Nullstellensatz, we know that $\mathfrak{p}_r = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ with $a_i \in k$. By Krull's theorem, we see that $h(\mathfrak{p}_r) \leq n$. It follows that $\dim k[X_1, X_2, \ldots, X_n] = n$. □

Let $I \subset k[X_1, X_2, \ldots, X_n]$ be prime ideal. We let $V = \mathcal{V}(I) \subset k^n$ the irreducible affine variety. We have $I(V) = \sqrt{I} = I$. Thus, the algebraic functions on V is $A = k[X_1, X_2, \ldots, X_n]/I$. In this setting, we defined $\dim V := \deg HP_I(t)$. On the other hand, one may ask how does this compare to $\dim A$? Indeed, we have $\dim V = \dim A$. To see this, first, by the Noether normalisation theorem, we know that there exist algebraically independent elements $a_1, a_2, \ldots, a_d$ such that $A \supset k[a_1, a_2, \ldots, a_d]$ is integral. Moreover, by Proposition 4.26, we have $d = \dim V$. The Corollary 6.20 showed that $\dim k[a_1, a_2, \ldots, a_d] = d$. Finally, to conclude that $\dim V = \dim A$, we need the following theorem.

Theorem 6.21. *(Cohen-Seidenberg) Let $A \subset B$ rings such that B is integral over A.*

(1) (Lying-over) For all prime ideals $\mathfrak{p} \subset A$, there exists a prime ideal $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. In other words, the canonical map $\mathrm{Spec}B \to \mathrm{Spec}A$ *is surjective.*

(2) If $\mathfrak{q}_1, \mathfrak{q}_2 \subset B$ are two prime ideals such that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap B$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$ then $\mathfrak{q}_1 = \mathfrak{q}_2$.

(3) (Going up) $\dim A = \dim B$.

We will need the following lemma in the proof:

Lemma 6.22. *Let $A \subset B$ rings such that B is integral over A.*

(i) Let I be an ideal in B and $I_A = I \cap A$ be the ideal in A. Then B/I is integral over A/I_A.
(ii) Let S be a multiplicative set in A, which we also view as a multiplicative set in B. Then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. Let $b \in B$, then there exist $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1b + a_0 = 0$$

(i) Apply the homomorphism $\bar{\ } : B \to B/I$, to deduce that $\bar{b}$ is integral over A/I_A.

(ii) Let $s \in S$, then we can use the above equation to deduce

$$\frac{b^n}{s^n} + \frac{a_{n-1}}{s}\frac{b^{n-1}}{s^{n-1}} + \ldots + \frac{a_1}{s^{n-1}}\frac{b}{s} + \frac{a_0}{s^n} = 0$$

from which we see that b/s is integral over $S^{-1}A$. □

◁ Show that if B is integral over A, then the canonical map $\mathrm{Spec}B \to \mathrm{Spec}A$ sends maximal ideals to maximal ideals.

Proof. (of Cohen-Seidenberg) Let $S = A \setminus \mathfrak{p}$ be the multiplicatively closed set. By Lemma 6.22, the local ring $S^{-1}B$ is an integral extension of the local ring $S^{-1}A$. Furthermore, the prime ideals $\mathfrak{q}$ of B lying over the prime ideal $\mathfrak{p}$ of A, that is $\mathfrak{q}$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ correspond bijectively with the maximal ideals of $S^{-1}B$ lying over the maximal ideal $S^{-1}\mathfrak{p}$ of $A_{\mathfrak{p}}$. Hence, for the proof of (1) and (2), we may assume that $\mathfrak{p}$ is a maximal ideal in A.

To prove that there exists a maximal ideal $\mathfrak{q}$ over a given maximal ideal $\mathfrak{p}$ of A, it suffices to prove that $\mathfrak{p}B \neq B$. For then any maximal ideal $\mathfrak{q}$ of B containing $I \coloneqq \mathfrak{p}B$ satisfies $\mathfrak{q} \cap A \subset \mathfrak{p}$ but since $1 \notin \mathfrak{q} \cap A$, it follows that $\mathfrak{q} \cap A = \mathfrak{p}$.

Suppose for contradiction that $\mathfrak{p}B = B$. Then, $1 = \sum_{i=1}^{r} p_i b_i$ with $p_i \in \mathfrak{p}$ and $b_i \in B$. Since $B \supset A$ is integral, all the $b_i \in B$ are integral over A. Therefore, $C \coloneqq A[b_1, b_2, \ldots, b_r]$ is integral over A and $\mathfrak{p}C = C$. Let $C = Ac_1 + Ac_2 + \ldots + Ac_n$ with $c_i \in C$. Then we can write

$$c_i = \sum_{j=1}^{n} p_{ij} c_j \text{ for } \ p_{ij} \in \mathfrak{p}$$

Consider the n-by-n matrix N with entries p_{ij} and c be the column matrix with entries c_i. Then, we have $Nc = c$, or equivalently $(N - I_n)c = 0$. By Cramer's rule applied to $M = N - I_n$, we get that $c_i det(N - I_n) = 0$ for all i. Since $1 \in C$, we can write $1 = \sum_{i=1}^{n} a_i c_i$ and so it follows that $\det(N - I_n) = \sum_{i=1}^{n} a_i c_i \det(N - I_n) = 0$. Thus, this gives that the polynomial

$$p(x) = \det(N - xI_n) = x^n + u_{n-1}x^{n-1} + \ldots + u_1 x + u_0, \text{ with } \ u_i \in \mathfrak{p}$$

is a monic polynomial with $p(1) = 0$ but all the non-leading coefficients are in $\mathfrak{p}$, hence this implies that $1 \in \mathfrak{p}$, which is a contradiction.

Finally, we prove that $\dim A = \dim B$. Suppose $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n \subsetneq B$ is a a chain of prime ideals. Then $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ and the corresponding chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n \subsetneq A$ has the same length by part (2). Thus, it follows that $\dim B \leq \dim A$.

Conversely, suppose that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n \subsetneq A$ be a chain of prime ideals in A. By part (1), we can construct a prime ideal $\mathfrak{q}_0$ in B lying over $\mathfrak{p}_0$. Suppose for induction that we have already constructed a chain of prime ideals, $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_i$ such that $\mathfrak{q}_j \cap A = \mathfrak{p}_j$ for $j \leq i$. We want to construct a prime ideal $\mathfrak{q}_{i+1} \supset \mathfrak{q}_i$ such that $\mathfrak{q}_{i+1} \cap A = \mathfrak{p}_{i+1}$. By Lemma 6.22 (i) $B/\mathfrak{q}_i$ is integral over $A/\mathfrak{p}_i$. Consider the prime ideal $\mathfrak{p}_{i+1}/\mathfrak{p}_i$ in $A/\mathfrak{p}_i$. By part (1), there exists a prime ideal $\mathfrak{q}_{i+1}/\mathfrak{q}_i$ in $B/\mathfrak{q}_i$ lying over $\mathfrak{p}_{i+1}/\mathfrak{p}_i$. Hence, $\mathfrak{q}_{i+1}$ is a prime ideal in B with $\mathfrak{q}_{i+1} \cap A = \mathfrak{p}_{i+1}$ and the proof is complete. □

7 Valuation rings

Definition 7.1. *Let R be an integral domain and K be its field of fractions. We say that R is a* **valuation ring** *if for all $x \in K \setminus \{0\}$, either $x \in R$ or $x^{-1} \in R$.*

Obviously, K itself is a valuation ring. Here is a more interesting example. Let p be a prime number and consider the ring

$$\mathbb{Q}_{(p)} \coloneqq \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$$

Thus $\mathbb{Q}_{(p)}$ is a subring of $\mathbb{Q}$ with field of fractions $\mathbb{Q}$. More generally, let R be a UFD with K as its field of fractions, and $\pi \in R$ a prime element. Then,

$$R_{(\pi)} \coloneqq \{\frac{a}{b} : a, b \in R, \pi \nmid b\}$$

is a valuation ring.

Note that it is obvious from the definition that if $R \subset K$ is a valuation ring with field of fractions K, and R' is another ring such that $R \subset R' \subset K$, then R' is also a valuation ring with K as the field of fractions.

Proposition 7.2. *Let R be a valuation ring with field of fractions K.*

(i) If I and J are ideals in R, then either $I \subset J$ or $J \subset I$.

(ii) R is a local ring with maximal ideal $\mathfrak{m}_R$.

(iii) $K \setminus R = \{x \in K \setminus \{0\} : x^{-1} \in \mathfrak{m}\}$.

Proof. (i) Suppose that there exists $x \in I$ such that $x \notin J$, we have to show that $J \subset I$. Let $0 \neq y \in J$, then $xy^{-1} \notin R$ (otherwise, $x = y(xy^{-1})$ contradiction). Hence, $x^{-1}y \in R$. So, $y = x(x^{-1}y) \in I$.

(ii) Let $x, y \in R$ non-units. Then $(x), (y) \subset R$ are proper ideals. From part (i), we have either $(x) \subset (y)$ or $(y) \subset (x)$. Say, $(y) \subset (x)$, then $x \pm y, xy \in (x)$ are non-units. Therefore, $\mathfrak{m}_R \coloneqq \{x \in R : x \text{ non-unit }\}$ is an ideal. Thus, R is a local ring with $\mathfrak{m}_R$ as its maximal ideal.

(iii) Let $x \in K \setminus R$. Then $x \neq 0$ and $x^{-1} \in R$. If $x^{-1} \notin \mathfrak{m}_R$ then x^{-1} is invertible in R, hence $x = (x^{-1})^{-1} \in R$, a contradiction. Thus, $x^{-1} \in \mathfrak{m}_R$. Conversely, let $x \in K \setminus \{0\}$ such that $x^{-1} \in \mathfrak{m}_R$. If $x \in R$, then $1 = xx^{-1} \in \mathfrak{m}_R$, contradiction. So, $x \notin R$. □

Theorem 7.3. *Let K be a field, $A \subset K$ be a subring, and $\mathfrak{p} \subset A$ a prime ideal. Then, there exists a valuation ring $R \subset K$ such that $A \subset R$ and $\mathfrak{p} = \mathfrak{m}_R \cap A$.*

Proof. By considering $A_{\mathfrak{p}}$, the localisation at the prime ideal $\mathfrak{p}$, it suffices to show the theorem for $A_{\mathfrak{p}}$ with its maximal ideal $\mathfrak{m}_{\mathfrak{p}}$. Therefore, without loss of generality, we assume that A itself is a local ring and $\mathfrak{p}$ is its maximal ideal.

Let us define $\mathcal{F} \coloneqq \{B \subset K : B \text{ subring}, \ A \subset B \text{ and } 1 \notin \mathfrak{p}B\}$. We have $A \in \mathcal{F}$. If $\{B_\lambda\}_{\lambda \in \mathcal{T}}$ is a family of elements in $\mathcal{F}$ that is totally ordered with respect to inclusion ($\lambda, \mu \in \mathcal{T} : B_\lambda \subset B_\mu$ or

$B_\mu \subset B_\lambda$) then $\bigcup_{\lambda\in\mathcal{T}} B_\lambda \in \mathcal{F}$ and is an upperbound for the family. Hence, we can apply Zorn's lemma and find a maximal element $R \in \mathcal{F}$ with respect to inclusion. We have $\mathfrak{p}R \neq R$, hence there exists $\mathfrak{m}_R \subset R$ a maximal ideal such that $\mathfrak{p}R \subset \mathfrak{m}_R$. Now, the localisation $R_{\mathfrak{m}_R}$ contains R (as R is an integral domain) but also $R_{\mathfrak{m}_R} \in \mathcal{F}$. Hence, it must be that $R = R_{\mathfrak{m}_R}$. Therefore, R is a local ring with maximal ideal $\mathfrak{m}_R$. As $\mathfrak{p} \subset \mathfrak{m}_R$, we have that $\mathfrak{p} \subset A \cap \mathfrak{m}_R$, but $\mathfrak{p}$ is a maximal ideal in A, hence $\mathfrak{p} = A \cap \mathfrak{m}_R$.

It remains to show that R is a valuation ring. Let $0 \neq x \in K$ such that $x \notin R$. We want to see that $x^{-1} \in R$. Consider $R \subsetneq R[x] \subset K$. By the maximality of R, we have $R[x] \notin \mathcal{F}$. Hence, $1 \in \mathfrak{p}R[x]$. Thus, we can write

$$1 = a_0 + a_1 x + \ldots + a_n x^n \text{ with } \ a_i \in \mathfrak{p}R \subset \mathfrak{m}_R$$

We have $1 - a_0 \notin \mathfrak{m}_R$, hence $1 - a_0$ is invertible in R. Therefore, we also have a relation

$$1 = b_1 x + \ldots + b_n x^n \text{ with } b_i \in \mathfrak{m}_R$$

Among such relations choose the one which has the smallest n. Now, suppose that $x^{-1} \notin R$. By the same argument, we get an equation

$$1 = c_1 x^{-1} + \ldots + c_m x^{-m} \text{ with } c_i \in \mathfrak{m}_R$$

and m minimal. Now either $n \geq m$ or $n < m$. Let's suppose $n \geq m$. Then, multiplying the last equation with $b_n x^n$, we have

$$b_n x^n = b_n c_1 x^{n-1} + \ldots + b_n c_m x^{n-m}$$

we get

$$0 = -b_n x^n + b_n c_1 x^{n-1} + \ldots + b_n c_m x^{n-m}$$

adding this to $1 = b_1 x + \ldots + b_n x^n$ we get

$$1 = (b_n c_1 + b_{n-1}) x^{n-1} + \ldots + (c_m b_n - b_{n-m}) x^{n-m} + \ldots + b_2 x^2 + b_1 x$$

which contradicts to the minimaly of n. (If $n = m$, as before, we observe that $1 - c_m b_m$ is invertible in R so we can eliminate $c_m b_m$ term.)

Finally, if $n < m$, we can do the same argument in the other direction, to contradict the minimality of m. □

Theorem 7.4. *Let K be a field and $A \subset K$ subring.*

$$\bigcap_{A\subset R\subset K} R = \overline{A}_K = \{x \in K : x \text{ integral over } A\}$$

where the intersection is taken over all valuation rings R containing A with field of fractions K. Moreover, all the valuation rings $R \subset K$ are integrally closed in K.

Proof. Let $R \subset K$ be a valuation ring and $x \in K$ be integral over R. Suppose $x \notin R$. Then, there exists $m \geq 1$, $a_i \in R$ such that

$$x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 = 0.$$

Since R is a valuation ring and $x \in K \setminus R$, we have $x^{-1} \in \mathfrak{m}_R$. Thus, we get

$$1 + a_{m-1}x^{-1} + \ldots + a_1 x^{1-m} + a_0 x^{-m} = 0$$

But, this implies $1 \in \mathfrak{m}_R$, which is a contradiction. Hence, $x \in R$. This gives us $\overline{A}_K \subset \bigcap_{A \subset R \subset K} R$.

Conversely, let $x \in K$ and suppose that x is not integral over A. We must show that there exists a valuation ring $R \subset K$ and $A \subset R$ such that $x \notin R$. We claim that the ideal $x^{-1}A[x^{-1}] \subset A[x^{-1}]$ does not contain 1. Indeed, if $1 \in x^{-1}A[x^{-1}]$, then

$$1 = a_1 x^{-1} + \ldots + a_n x^{-n} \text{ with } a_i \in A$$

Multiplying with x^n gives

$$x^n = a_1 x^{n-1} + \ldots + a_n$$

which implies x is integral over A, a contradiction. Thus, there exists a maximal ideal $\mathfrak{m} \subset A[x^{-1}]$ with $x^{-1}A[x^{-1}] \subset \mathfrak{m}$.

Now, by Theorem 7.3, there exist a valuation ring $R \subset K$ with $A[y] \subset R$ and $\mathfrak{m}_R \cap A[y] = \mathfrak{m}$. Therefore, $x^{-1} \in \mathfrak{m}_R$. Hence, $x \in K \setminus R$ as desired. □

You may wonder why are the valuation rings are called valuation rings. What are the "valuations" on them?

Definition 7.5. *An* **ordered group** Γ *is an abelian group with a total order* $\leq$ *compatible with the addition law, in the sense that* $a \leq b$ *and* $c \leq d$ *implies* $a + c \leq b + d$ *for all* $a, b, c, d \in \Gamma$.

Examples are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with the usual order and $\mathbb{Z} \oplus \mathbb{Z}$ with the lex order.

Definition 7.6. *Let* K *be a field and* Γ *an ordered group. A map* $\nu : K \to \Gamma \cup \{\infty\}$ *is called a valuation of* K *if*

(1) $\nu(xy) = \nu(x) + \nu(y)$, *for all* $x, y \in K$,

(2) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,

(3) $\nu(x) = \infty$ *if and only if* $x = 0$.

It is quite easy to verify that the subset $R_\nu := \{x \in K : \nu(x) \geq 0\}$ is a valuation ring and $\mathfrak{m}_\nu = \{x \in K : \nu(x > 0\}$ is its maximal ideal.

Proposition 7.7. *Let* $R \subset K$ *be a valuation ring, then there exists and ordered group* Γ *and a valuation* $\nu : K \to \Gamma \cup \{\infty\}$ *such that* $R = R_\nu$.

Proof. Given a valuation ring $R \subset K$, let us define the abelian group

$$\Gamma \coloneqq \{xR : x \in K \setminus \{0\}\}$$

with addition $xR + yR = xyR$. We define a total order on Γ by setting $xR \leq yR$ if and only if $yR \subset xR$. We can then define a valuation $\nu : K \to \Gamma \cup \{\infty\}$ by setting $\nu(x) = xR$. It is then easy to verify that $R = R_\nu$ and $\mathfrak{m}_R = \mathfrak{m}_\nu$. □

We next want to understand valuation rings that are Noetherian.

Theorem 7.8. *Let R be a valuation ring in K. Then, the following are equivalent:*

(1) R is a **discrete valuation ring** *(DVR), that is, there exists a surjective valuation $\nu : K \to \mathbb{Z} \cup \{\infty\}$ such that $R_\nu = R$,*

(2) R is a principal ideal domain,

(3) R is Noetherian.

Theorem 7.9. *Let R be a ring. The following are equivalent*

(1) R is a discrete valuation ring,

(2) R is a local principal ideal domain and not a field.

(3) R is Noetherian, local, $\dim R > 0$ *and its maximal ideal is principal,*

(4) R is Noetherian, local, normal and $\dim R = 1$.

Definition 7.10. *A Noetherian, normal ring of dimension 1 is called a* **Dedekind domain**.

I used the following references when preparing these lecture notes. This subject is a classical topic. Nothing I wrote is original.

References

[1] Cox, Little, O'Shea - Ideals, Varieties, and Algorithms

[2] Reid - Undergraduate Commutative Algebra

[3] Atiyah, Macdonald - Introduction to Commutative Algebra

[4] Matsumura - Commutative Ring Theory

[5] Kunz - Introduction to Commutative Algebra and Algebraic Geometry

[6] Schenk - Computational Algebraic Geometry

[7] Arrondo - The Nullstellensatz without the Axiom of Choice. arXiv:2009.02837.