

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, Krull dimension, localisation, Artin rings, Krull's principal ideal theorem, Cohen-Seidenberg lying over/going up theorem, (Discrete) Valuation Rings, Artin-Rees lemma, Krull intersection theorem, Completion, Hensel's lemma.

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

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

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 . For example, $\mathbb{Z}[\xi]$ does not have this property for $n = 23$). 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 19th 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

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

bases and Buchberger's algorithm which simultaneously generalise Gaussian elimination in linear 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 is 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 $\text{Frac}(R)$ 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 .

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

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

A **homomorphism** of rings $f : R \rightarrow S$ 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 $|\cdot| : R \rightarrow \mathbb{N}$ 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 $f : R \rightarrow S$. 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 $I \subset R$, 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 $f : R \rightarrow R/I$ 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

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

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).

End of lec. 1

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.

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$$IJ = \left\{ \sum_{i=1}^t a_i b_i \mid a_i \in I, b_i \in J, t \in \mathbb{N} \right\}.$$

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 $I + J = (\text{gcd}(m, n))$.

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 $\pi : R/IJ = R/I \cap J \rightarrow R/I \times R/J$ 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, \dots, I_r are pairwise coprime ideals, that is, $I_i + I_j = R$ for $i \neq j$, then $I_1 I_2 \dots I_r = I_1 \cap I_2 \cap \dots \cap I_r$ and*

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

Proof. We proceed by induction on r . The case $r = 2$ is already established. Let us put $J = I_2 \dots I_r$. We want to show that $I_1 + J = R$. Since $I_1 + I_i = R$ for all $i \geq 2$, we can find elements $r_i \in I_1$ and $s_i \in I_i$ such that $r_i + s_i = 1$. Then, we obtain

$$1 = \prod_{i=1}^r (r_i + s_i) = r + s_2 s_3 \dots s_r$$

where r is a sum of terms each of which contains at least one r_i as a factor. Therefore, $r \in I_1$. As $s_2 s_3 \dots s_r \in J$, we see that $I_1 + J = R$. Now, we can deduce that

$$R/I_1 J \simeq R/I_1 \times R/J$$

and the result follows by induction. □

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

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

2.2.1 maximal, prime and \sqrt{r} radical ideals

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 proper ideals in R containing I . 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 $\mathbb{C}[X, Y] \rightarrow \mathbb{C}$ 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 $f : R_1 \rightarrow R_2$ 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 $f : \mathbb{Z} \rightarrow \mathbb{Q}$ 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 $f : R_1 \rightarrow R_2$ 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. \square

A multiplicative set S is called **saturated** if it is closed under taking divisors: i.e., whenever $xy \in S$, the elements x and y are in S too.

< Show that S is a saturated multiplicative set if and only if the complement of S is union of prime ideals (uses Zorn's lemma).

End of lec. 2

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

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

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 $S = \{1, x, x^2, \dots\}$. By the previous proposition, there exists a prime ideal containing I and not containing x . \square

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

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

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.

Proposition 2.9. (*Prime avoidance*) Suppose that I is an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, then $I \subset \mathfrak{p}_j$ for some j .

Proof. We argue by induction on n . Case $n = 1$ is trivial. For each i , choose $x_i \in I \setminus \bigcup_{i=1, i \neq j}^n \mathfrak{p}_i$. If no such x_i exists, we are done by induction. So assume $x_i \in I$ exists such that $x_i \in \mathfrak{p}_i$ and $x_i \notin \bigcup_{i=1, i \neq j}^n \mathfrak{p}_i$. Then consider the element

$$y = \sum_{i=1}^n x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$$

By construction, this is an element of I but it is not in \mathfrak{p}_i as $x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n \notin \mathfrak{p}_i$. This gives the desired contradiction. \square

2.3 Modules

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

$$\begin{aligned} (r_1 r_2)m &= r_1(r_2 m) \\ (r_1 + r_2)m &= r_1 m + r_2 m \\ r(m_1 + m_2) &= r m_1 + r m_2 \\ 1m &= m \end{aligned}$$

In other words, it is an abelian group 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. To a module M , we can associate an ideal via the annihilator construction

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

Given an ideal I , we can consider R/I as an R -module. For such modules, we have $I = \text{ann}(R/I)$. 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 $x_1, \dots, x_m \in M$ such that $M = R \cdot x_1 + R \cdot x_2 + \dots + R \cdot x_m$.

◁ 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 $R/\text{ann}(M)$.

For $m \in M$, we can also define an ideal $\text{ann}(m) := \{r \in R : rm = 0\}$. Then, by definition, $\text{ann}(M) = \bigcap_{m \in M} \text{ann}(m)$.

Proposition 2.10. *Let M an R -module. Let I be an ideal that is maximal in the set $\{\text{ann}(m) : 0 \neq m \in M\}$ of all annihilators of non-zero elements of M . Then I is prime.*

Proof. Say $I = \text{ann}(m)$ for some $m \in M$. Given $ab \in I$, suppose that $a \notin I$. Then $am \neq 0$. On the other hand, we have $\text{ann}(am) \supset I$. By hypothesis, it cannot be larger, hence $\text{ann}(am) = I$. Now, it follows that b annihilates am , hence $b \in I$. \square

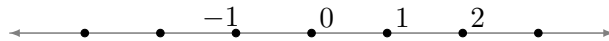
3 Examples

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.

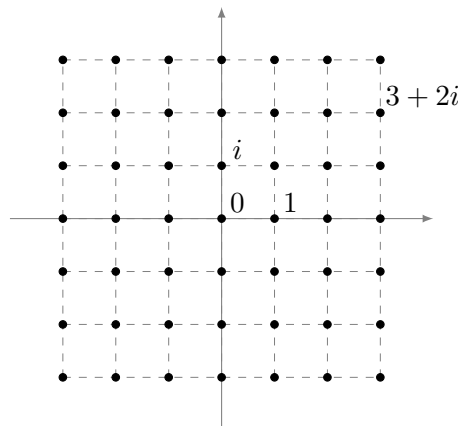
The most fundamental ring is \mathbb{Z} which you encountered in nursery. Prime ideals of \mathbb{Z} are (p) for p prime number and (0) .



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 simplest 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.).

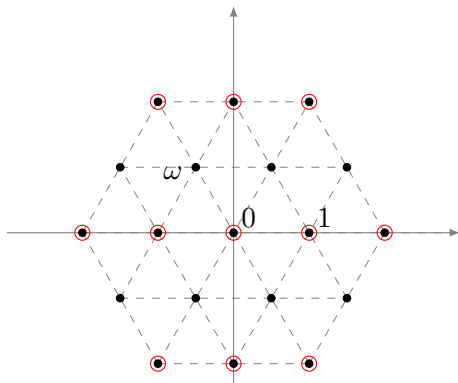


Figure 1: The elements of the ring $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$. The subring $\mathbb{Z}[\sqrt{-3}]$ is marked red.

< 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.

End of lec. 3

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

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$

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

$$R[X_1, \dots, X_n] = R[X_1] \cdots [X_n] = \left\{ \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n} \mid a_{i_1, \dots, i_n} \in R \right\},$$

where all but finitely many coefficients are equal to zero.

< Let k be an infinite field, and $f \in k[X_1, \dots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in k^n$. (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

$$R[[T]] = \{a_0 + a_1T + \dots \mid a_i \in R\}.$$

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

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

$k[X_1, \dots, X_n]$ is an integral domain, and a UFD. $k[X_1]$ is in fact a PID but $k[X_1, \dots, X_n]$ 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 $I = (X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, \dots, X^{i_t}Y^{j_t})$ 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:

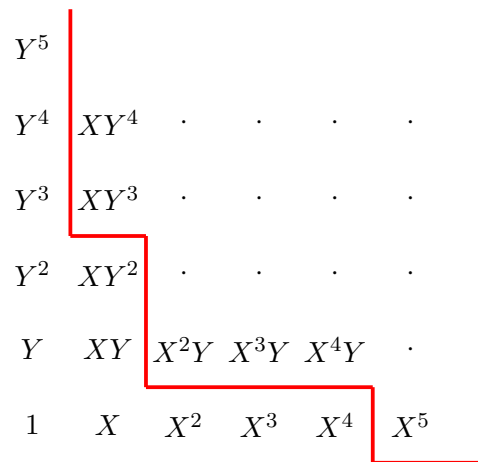


Figure 2: The monomial ideal $(XY^3, X^2Y, X^5) \subset k[X, Y]$.

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 $\mathbb{Z}[X]$.

< 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 $\bar{f} \in \mathbb{F}_p[X]$ 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 $\bar{f} \in \mathbb{F}_p[X]$ and then consider the ideal (p, f) where $f \in \mathbb{Z}[X]$ is any lift of \bar{f} to a polynomial in $\mathbb{Z}[X]$. (Check that $(p, f) = (p, g)$ if $\bar{f} = \bar{g} \in \mathbb{F}_p[X]$).

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

< 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 $f(X) = a_0 + a_1X + \dots$ with $a_0 \neq 0$.

Let $p \in \mathbb{Z}$ be a prime number, the ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\} \subset \mathbb{Q}$ 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 $k[X_1, X_2, \dots, X_n]$

4.1 Hilbert basis theorem

Theorem 4.1. $k[X_1, X_2, \dots, X_n]$ 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

$$I_1 \subset I_2 \subset I_3 \dots$$

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 $I = (f_1, f_2, \dots, f_m)$ 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

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

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

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

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

➤ 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

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

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

$$J_0 \subset J_1 \subset \dots$$

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 $J_m = (a_{m,1}, a_{m,2}, \dots, a_{m,r_m})$. 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 $\{f_{m,j}\}_{0 \leq m \leq s, 1 \leq j \leq r_m}$. \square

► Not every subring of a Noetherian ring is Noetherian.

< Show that

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

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

4.2 Affine varieties

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

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

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

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

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

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

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

$$\{S \subset k[X_1, \dots, X_n]\} \begin{matrix} \xrightarrow{\mathcal{V}} \\ \xleftarrow{\mathcal{I}} \end{matrix} \{U \subset k^n\}$$

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

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 $k[X_1, \dots, X_n]$. Let us introduce some notation.

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

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

We write an element $f \in k[X_1, \dots, X_n]$ 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

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

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

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

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

\triangleleft 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 $k[X_1, \dots, X_n]$ by setting $\beta \leq_A \alpha$ if and only if $A\beta \leq_{lex} A\alpha$. In fact, any monomial ordering on $k[X_1, X_2, \dots, X_n]$ 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

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

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

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

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

³L Robbiano - Term orderings on the polynomial ring.

Lemma 4.4. Let $I \subset k[X_1, \dots, X_n]$ be a monomial ideal generated by a set G of monomials and $f \in k[X_1, \dots, X_n]$ 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 $h_i \in k[X_1, \dots, X_n]$ 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. \square

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

Proof. Let $I = (g_i : i \geq 1)$. By Hilbert's basis theorem, there exists r such that $I = (g_1, \dots, g_r)$. 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 $j \in \{1, \dots, r\}$ such that $g_j | g_i$. Hence, $g_r \leq g_j \leq g_i$ hence $g_i = g_r$. \square

End of lec. 5

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

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

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 $LT(r) \leq LT(f)$

Proof. Suppose that there exists an i such that $LT(f_i) | LT(f)$ and let $i \in \{1, \dots, s\}$ be the smallest index 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

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

with the required conditions. Then we can write

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

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 not 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 $\tilde{f} = h_1 f_1 + \dots + h_s f_s + \tilde{r}$. Then, we set

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

where $r = \tilde{r} + LT(f)$. \square

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 $XY \mid XY^2$, we can write $\tilde{f} = f - Yf_1 = -X - Y$. Hence,

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

Another possibility is to use that $Y^2 \mid XY^2$, 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, \dots, 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

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

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

◁ 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 $\mathbf{in}(I)$.

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 $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of $I \subset k[X_1, \dots, X_n]$.

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

$$f = h_1g_1 + h_2g_2 + \dots + h_s g_s + r.$$

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, \dots, g_s .

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

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

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

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 $LT(\tilde{r} - r) \in \text{in}(I) = (LT(g) : g \in G)$. 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, $k[X_1, \dots, X_n]/I$ 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, \dots, g_s , we get

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

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. □ End of lec. 6

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

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

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. \square

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 $f, g \in k[X_1, \dots, X_n]$ be nonzero polynomials. Let $X^\alpha = LM(f)$ with $\alpha = (\alpha_1, \dots, \alpha_n)$ and $X^\beta = LM(g)$ with $\beta = (\beta_1, \dots, \beta_n)$. Define $\gamma = (\gamma_1, \dots, \gamma_n)$ with $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all i , i.e. $X^\gamma = \text{lcm}(LM(f), LM(g))$. 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 $\text{lcm}(LM(f), LM(g)) = X^2YZ^2$, 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)
```

► $LM(S(f, g)) < \text{lcm}(LM(f), LM(g))$. 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 $I \subset k[X_1, \dots, X_n]$ be a non-zero ideal. $G = \{g_1, \dots, g_s\} \in I \setminus \{0\}$ such that $I = (g_1, \dots, g_s)$. 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 $\{g_1, \dots, g_s\}$ 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 $g_1, \dots, g_s \in k[X_1, \dots, X_n]$, $\alpha_1, \dots, \alpha_s \in \mathbb{N}^n$ and $c_1, \dots, c_s \in k \setminus \{0\}$. Let*

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

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 $\gamma_{ij} = \text{lcm}(LM(g_i), LM(g_j))$. Moreover, $LM(X^{\delta - \gamma_{ij}} S(g_i, g_j)) < X^\delta$.

Proof. 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, $X^{\gamma_{ij}} | X^\delta$. In particular, $X^{\delta - \gamma_{ij}} \in k[X_1, \dots, X_n]$.

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 compute

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

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

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

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 $LT(f) \in (LT(g_1), \dots, LT(g_s))$. Write

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

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

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

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

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

Now, by assumption, division by remainder gives

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

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 $u_i^* \in k[X_1, \dots, X_n]$ such that

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

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

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

Hence, we can write

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

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. \square

► Let $X^{\alpha_i} = LM(g_j)$ and $X^{\gamma_{ij}} = \text{lcm}(LM(g_i), LM(g_j))$. By definition, $S(g_i, g_j) = h_i g_i + h_j g_j$ where $h_i = X^{\gamma_{ij} - \alpha_i}$ and $h_j = X^{\gamma_{ij} - \alpha_j}$. It is a common mistake to conclude that the division with remainder of $S(g_i, g_j)$ by g_i, g_j has zero remainder. This is false in general - indeed the expression $h_i g_i + h_j g_j$ is not generally the result of the division with remainder algorithm. For example, by Theorem 4.11, this won't be the case for some $S(g_i, g_j)$ if $\{g_1, \dots, g_s\}$ is not a Gröbner basis.

End of lec. 7

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

Initialize with $G = \{f_1, \dots, f_t\}$. Now, suppose $G = \{g_1, \dots, g_s\}$. 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

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

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, $r = 0$. \square

► 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
```

\triangleleft (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 $I \subset k[X_1, \dots, X_n]$ be an ideal and $s \in \mathbb{N}$, and let us write

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

and

$$I_{\leq s} := I \cap k[X_1, \dots, X_n]_{\leq s}$$

We define

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

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

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

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

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

is a polynomial of degree n .

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

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

We have

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

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,

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

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

$$HF_I(s) = HF_{\mathbf{in}(I)}(s) \text{ for all } s \geq 0.$$

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

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

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

We will show that (a) $\{f_1, \dots, f_m\}$ is a k -basis of $I_{\leq s}$, (b) $\{LM(f_1), \dots, LM(f_m)\}$ gives a k -basis for $\mathbf{in}(I)_{\leq s}$. (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

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

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

Linear independence for (b): clear.

Spanning property 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' .

Spanning property for (b): Let $g \in \mathbf{in}(I)_{\leq s}$. Then $g = \sum_j h_j LT(g_j)$ for some $h_j \in k[X_1, \dots, X_n]$ and $g_j \in I$. We write $h_j = \sum_\alpha a_{\alpha,j} X^\alpha$ with $a_{\alpha,j} \in k$. Hence, $g = \sum_{j,\alpha} a_{\alpha,j} X^\alpha LT(g_j) = \sum_{j,\alpha} a_{\alpha,j} LT(X^\alpha g_j)$. Since $X^\alpha g_j \in I$, by letting $g_{\alpha,j} = X^\alpha g_j$, 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 $LM(f_1), \dots, LM(f_m)$. \square *End of lec. 8*

► 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, $\text{in}(I) = (X^2, XY, XZ, Y^3)$. 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 $HP_I(t) = 3t + 1$.

Theorem 4.16. *Let $I \subset k[X_1, \dots, X_n]$. 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*

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

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

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

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 $I = \text{in}(I) = (X^{\beta^{(1)}}, \dots, X^{\beta^{(m)}})$ 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 $C(I) := \{\alpha \in \mathbb{N}^n : X^{\beta^{(i)}} \mid X^\alpha \text{ for any } i\}$ and $C(I)_{\leq s} := \{\alpha \in \mathbb{N}^n : |\alpha| \leq s, \alpha \in C(I)\}$. 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 $J \subset \{1, 2, \dots, n\}$ and a function $\tau : J \rightarrow \mathbb{N}$, we set

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

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

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

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

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

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 $i \in \{1, \dots, n\}$ such that $\alpha_i < \beta_i$. Hence,

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

where in the last equality, we have avoided to specify which specific (J, τ) are used in order to avoid cumbersome notation. It suffices to note that there are only finitely many (J, τ) that are being used. Now, the claim follows from

$$C(I) = \bigcap_{i=1}^m C(\beta^{(i)}) = \bigcap_{i=1}^m \bigcup_{(J, \tau)} C(J, \tau) = \bigcup \{ \text{intersections of } C(J, \tau) \} = \bigcup_{(J, \tau) \in \mathcal{J}} C(J, \tau)$$

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

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

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

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

□

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 $I \subset k[X_1, \dots, X_n]$. If $V \neq \emptyset$, then $\mathcal{I}(V) \neq k[X_1, \dots, X_n]$ and $HP_{\mathcal{I}(V)} \neq 0$. We define

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

< 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 $I \subset k[X_1, \dots, X_n]$ be a proper ideal.*

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

In other words, this means that there exists d “algebraically independent” directions to project $V(I)$ by restricting $(X_{i_1}, X_{i_2}, \dots, X_{i_d})$ 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, $X^{\gamma + \alpha} = X^\gamma LT(f) \in \text{in}(I)$. But, this contradicts with $\gamma + \alpha \in C(I)$.

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

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

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

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

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

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

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

► We have seen before that the initial ideal of $I = (Y - X^2, Z - X^3) \subset k[X, Y, Z]$ with respect to \leq_{grlex} is given by $\text{in}(I) = (X^2, XY, XZ, Y^3)$. Now, it is clear that $\text{in}(I) \cap k[Z] = \{0\}$ and $\text{in}(I) \cap k[X, Z]$, $\text{in}(I) \cap k[Y, Z]$ and $\text{in}(I) \cap k[X, Y]$ are all non-trivial. Hence $\dim V(I) = 1$.

◁ For $I = (Y - X^2, Z - X^3) \subset k[X, Y, Z]$. Show directly that $I \cap k[X, Y]$, $I \cap k[X, Z]$ and $I \cap k[Y, Z]$ are non-trivial.

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.

End of lec. 9

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, $\mathcal{V}(I) = \emptyset$ 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 analogous statement holds in the case of a polynomial ring with many variables.

Theorem 4.19. (*Weak Nullstellensatz*) *If k is algebraically closed, and $I \neq k[X_1, \dots, X_n]$ 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 $a_0, a_1, \dots, a_{m-1} \in A$ such that*

$$b^m + a_{m-1}b^{m-1} + \dots + a_1b + a_0 = 0$$

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.

End of lec. 10

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

- i. b is integral over A .*
- ii. $A[b] := \{f(b) : f \in A[X]\}$ 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 $M = [m_1 \ m_2 \ \dots \ m_n]$ where m_i are column vectors. Then the n linear equations can be written as

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

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

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

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, $A[b] = \{r(b) : r = 0 \text{ or } \deg(r) < m\} = A \cdot 1 + A \cdot b + \dots + A \cdot b^{m-1}$.

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

iii. implies i. : We have $C = Ac_1 + Ac_2 + \dots + Ac_n$ 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 $p(b) = 0$. \square

► 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 $B = A[b_1, \dots, b_n]$ with $b_i \in B$ such that b_i are integral over $A[b_1, \dots, b_{i-1}]$ for all i . Then B is integral over A and B is finitely generated as an A -module.*
- (b) *The integral closure $\bar{A}_B := \{b \in B : b \text{ integral over } A\}$ 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) Let $B = A[b, b']$ and b' is integral over $A[b]$ and b is integral over A . Then by Lemma 4.21, we see that $A[b]$ is a finitely generated A -module, and $A[b, b']$ is a finitely generated $A[b]$ -module. It follows that $A[b, b']$ is finitely generated as an A -module. Then, again by Lemma 4.21, it follows that B is integral over A . The general case follows from this 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 .

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

$$b^m + c_{m-1}b^{m-1} + \dots + c_1b + c_0 = 0 \text{ for some } c_0, \dots, c_{m-1} \in C$$

Let $C' = A[b, c_0, \dots, c_{m-1}] \subset B$. The ring $A[c_0, \dots, c_{m-1}]$ 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

$$a^{-n} + a_{n-1}a^{-n+1} + \dots + a_0 = 0, \text{ with } a_i \in A$$

Then, we have $a^{-1} = -(a_{n-1} + a_{n-2}a + \dots + a_0a^{n-1}) \in A$.

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

$$b^m + a_{m-1}b^{m-1} + \dots + a_1b + a_0 = 0 \text{ with } a_i \in A$$

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

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

□

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: $A \subset \text{Frac}(A)$. 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 $\text{Frac}(A)$ is called the **normalisation** of A .

► The ring $k[X_1, \dots, X_n]$ 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 $t = y/x \in \text{Frac}(A)$ 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 $k[X_1, \dots, X_n]$ or more generally a quotient ring $A = k[X_1, \dots, X_n]/I$ 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 $a_1, \dots, a_n \in A$ such that $A = \{f(a_1, \dots, a_n) : f \in k[X_1, \dots, X_n]\}$. We write $A = k[a_1, \dots, a_n]$. In this case, we have a surjective homomorphism

$$\pi : k[X_1, \dots, X_n] \rightarrow A$$

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

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 $A[X_1, \dots, X_n]/I$ for some n and ideal I in which case we can write $B = A[b_1, \dots, b_n]$ 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, \dots, a_n are **algebraically independent** if there is no non-zero polynomial $F \in k[X_1, \dots, X_n]$ such that $F(a_1, \dots, a_n) = 0$. This is equivalent to the injectivity of the homomorphism π .

End of lec.11

Theorem 4.25. (Noether normalisation⁴ lemma) *Let A be a finitely generated k -algebra. Then there exists $a_1, \dots, a_d \in A$ such that*

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

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

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

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 $A = k[x_1, \dots, x_n]$ for some $x_i \in A$. Suppose that x_1, \dots, x_n are algebraically dependent over k , and let $f(x_1, \dots, x_n) = 0$ be a relation, where $f \in k[X_1, \dots, X_n]$ is a non-constant polynomial. Write m for the degree of f , and let $f_m(X_1, \dots, X_n)$ be the homogeneous part of f of degree m . Take $c_1, \dots, c_{n-1} \in k$ such that $f_m(c_1, \dots, c_{n-1}, 1) \neq 0$. (It is at this step that we use k is infinite.) We now make a substitution by letting $y_i = x_i - c_i x_n$ for $i = 1, \dots, n - 1$. Then, we have

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

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

⁴Although 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.

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

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

where $N(\alpha) = (\sum_{i=1}^{n-1} r_i \alpha_i) + \alpha_n$ and $g_i^\alpha \in k[y_1, \dots, y_{n-1}]$. 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 $\alpha \rightarrow N(\alpha)$ 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 $\alpha = (\alpha_1, \dots, \alpha_n)$ with $a_\alpha \neq 0$ and letting $r_i = r^{n-i}$ so that $N(\alpha) = r^{n-1} \alpha_1 + r^{n-2} \alpha_2 + \dots + r \alpha_{n-1} + \alpha_n$. Then, we have

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

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

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 $A = k[X_1, \dots, X_n]/\mathcal{I}(V)$ be the finitely generated k -algebra of polynomial functions on V . Noether normalisation gives a subring $k[Y_1, \dots, Y_d] \subset A$ over which A is integral. For k algebraically closed, this implies that the corresponding map of varieties $\pi : V \rightarrow k^d$ 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

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

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

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

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

given by sending $F(y_1, y_2, \dots, y_d) \in k[Y_1, Y_2, \dots, Y_d]_{\leq s}$ to $\overline{F(f_1, f_2, \dots, f_d)} \in k[X_1, \dots, X_n]_{\leq Ns} / I_{\leq Ns}$. We claim that this map is injective. Indeed, suppose that $\overline{F(f_1, f_2, \dots, f_d)} \in I_{\leq Ns}$. This means that $\overline{F(f_1, f_2, \dots, f_d)} = \overline{F(\bar{f}_1, \bar{f}_2, \dots, \bar{f}_d)} = 0$ in A . But since $\bar{f}_1, \dots, \bar{f}_d$ are algebraically independent, it follows that $F = 0$. Therefore,

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

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

► 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 algebraically 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 , $K = \text{Frac}(A)$, and it is easy to see that if $\{a_1, \dots, a_d\}$ is a maximal set of algebraically independent elements in A , then we have the corresponding field extensions

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

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 $k \subset \text{Frac}(A)$, where $A = k[X_1, \dots, X_n]/\mathcal{I}(V)$.*

End of lec. 12

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 $k[X_1, \dots, X_n]$ are exactly of the form*

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

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

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

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

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

Conversely, suppose $\mathfrak{m} \subset k[X_1, \dots, X_n]$ is a maximal ideal. Then $A = k[X_1, \dots, X_n]/\mathfrak{m}$ is a field that is a finitely generated k -algebra. Applying Noether's normalisation, we can find $u_1, \dots, u_d \in A$ which are algebraically independent such that the extension $A \supset k[u_1, \dots, u_d]$ is integral. But, A is a field, therefore $k[u_1, \dots, u_d]$ is a field by Corollary 4.22 (d). Now, $k[u_1, \dots, u_d]$ 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 X_i under the isomorphism $k[X_1, \dots, X_n]/\mathfrak{m} \simeq k$, we see that $X_i - a_i \in \mathfrak{m}$. Hence,

$$(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n) \subset \mathfrak{m}$$

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

$$\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n).$$

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, \dots, a_n such that

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

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

► 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 unsatisfactory⁵. Let us remark that Proposition 2.4 was proved for a general commutative ring. The above theorem is concerned with the ring $k[X_1, \dots, X_n]$ 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 [8] which avoids any choice.

Theorem 4.30. (*Nullstellensatz without choice*) *Let k be any field. Any proper ideal $I \subset k[X_1, X_2, \dots, X_n]$ 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 $I \subset k[X_1, \dots, X_n]$ a proper ideal containing a polynomial g that is monic in X_n , thus*

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

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

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

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

$$R = \left(\begin{array}{cccccccc} f_0 & f_1 & \dots & f_e & 0 & 0 & \dots & 0 \\ 0 & f_0 & \dots & f_{e-1} & f_e & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & f_0 & f_1 & \dots & f_{e-1} & f_e \\ g_0 & g_1 & \dots & g_{d-1} & 1 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{d-2} & g_{d-1} & 1 & 0 \dots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{d-1} & 1 \end{array} \right) \left. \begin{array}{l} \vphantom{\begin{array}{c} \\ \\ \\ \\ \end{array}} \right\} d \text{ rows} \\ \left. \begin{array}{l} \vphantom{\begin{array}{c} \\ \\ \\ \end{array}} \\ \vphantom{\begin{array}{c} \\ \\ \end{array}} \end{array} \right\} e \text{ rows} .$$

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

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:

$$R = \left(\begin{array}{cccccccc} f & f_1 & \dots & f_e & 0 & 0 & \dots & 0 \\ X_n f & f_0 & \dots & f_{e-1} & f_e & 0 & \dots & 0 \\ & \ddots & & & & & & \\ X_n^{d-1} f & \dots & 0 & f_0 & f_1 & \dots & f_{e-1} & f_e \\ g & g_1 & \dots & g_{d-1} & 1 & 0 & \dots & 0 \\ X_n g & g_0 & \dots & g_{d-2} & g_{d-1} & 1 & 0 \dots & 0 \\ & & \ddots & & & & \ddots & \\ X_n^{e-1} g & \dots & 0 & g_0 & g_1 & \dots & g_{d-1} & 1 \end{array} \right) \begin{array}{l} \left. \vphantom{\begin{array}{c} f \\ X_n f \\ \dots \\ X_n^{d-1} f \\ g \\ X_n g \\ \dots \\ X_n^{e-1} g \end{array}} \right\} d \text{ rows} \\ \left. \vphantom{\begin{array}{c} f_0 \\ f_1 \\ \dots \\ f_{e-1} \\ f_e \\ g_0 \\ g_1 \\ \dots \\ g_{d-1} \\ 1 \end{array}} \right\} e \text{ rows} \\ . \end{array}$$

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

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 that g is monic with respect to X_n . So, we can assume that I contains such a g as in Lemma 4.31. Now, consider $I' = I \cap k[X_1, \dots, X_{n-1}]$. 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 $k' = k[X_1, \dots, X_{n-1}]/\mathfrak{m}'$. Consider the surjective homomorphism $\pi : k'[X_n] \rightarrow k[X_1, X_2, \dots, X_n]/(I + (\mathfrak{m}'))$. We have the isomorphism of rings

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

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

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.

End of lec. 13

Theorem 4.32. (Nullstellensatz - Strong form) Suppose that k is algebraically closed. $I \subset k[X_1, \dots, X_n]$ 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, $f^\ell(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in \mathcal{V}(I)$. But then, $f(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in \mathcal{V}(I)$. Thus, $f \in \mathcal{I}(\mathcal{V}(I))$.

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

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

For this, consider the polynomial ring $k[X_1, \dots, X_n, Y]$ and the ideal $\tilde{I} = (f_1, \dots, f_s, 1 - Yf) \subset k[X_1, \dots, X_n, Y]$. We will show that $\tilde{I} = k[X_1, \dots, X_n, Y]$. 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 $a_1, a_2, \dots, a_{n+1} \in k$ such that $\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n, Y - a_{n+1})$. Thus, for all $i = 1, \dots, s$, $f_i(a_1, \dots, a_n) = 0$. Therefore, $f(a_1, \dots, a_n) = 0$. But we also have $1 - fY \in \mathfrak{m}$ which gives

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

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

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

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

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

Choose ℓ sufficiently large so that $h_i(X_1, \dots, X_n) := f^\ell g_i(X_1, \dots, X_n, \frac{1}{f}) \in k[X_1, \dots, X_n]$ 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

$$\text{affine varieties} \begin{array}{c} \xrightarrow{\mathcal{I}} \\ \xleftarrow{\mathcal{V}} \end{array} \text{radical ideals}$$

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

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

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

□

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 $(f_1, \dots, f_s, 1 - Yf)$.

< 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 $k[X_1, \dots, X_n]$. 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 $1 \leq i_1 < i_2 < \dots < i_d \leq n$ such that $I \cap k[X_{i_1}, X_{i_2}, \dots, X_{i_d}] = \{0\}$. It suffices to show that

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

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

Corollary 4.35. *Let k be algebraically closed. $I \subset k[X_1, X_2, \dots, X_n]$ 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, the maximal ideals containing I are precisely the ones of the form $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ for some $(a_1, \dots, a_n) \in \mathcal{V}(I)$. Therefore, f vanishes on all $(a_1, \dots, a_n) \in \mathcal{V}(I)$. Hence, by the strong Nullstellensatz $f \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. \square

The last corollary implies that the ring $k[X_1, \dots, X_n]$ 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 radical 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 $k[X_1, \dots, X_n]/I$: 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 $k[X_1, \dots, X_n]$. Then, there exist prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r \in k[X_1, \dots, X_n]$ such that*

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

Moreover,

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

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 $f, g \in k[X_1, \dots, X_n]$ 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 $g \in \mathcal{I}(V)$. \square

Proof. (of Corollary 4.36) We first show that $V = \mathcal{V}(I)$ can be written as a union $V = V_1 \cup V_2 \cup \dots \cup V_r$ 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 (otherwise 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

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \dots$$

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

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

But, this contradicts the fact that $k[X_1, \dots, X_n]$ is Noetherian. Therefore, $V = V_1 \cup V_2 \cup \dots \cup V_r$ 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 $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r$ 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

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

Let $d := \deg HP_{\sqrt{I}}(t)$ and suppose that $\deg HP_{\mathfrak{p}_i}(t) < d$ for all i . Then, there exist $1 \leq i_1 < i_2 < \dots < i_d \leq n$ such that $\sqrt{I} \cap k[X_{i_1}, \dots, X_{i_d}] = \{0\}$ and $f_i \in \mathfrak{p}_i \cap k[X_{i_1}, \dots, X_{i_d}] \neq \{0\}$ for all i . We have $f = f_1 f_2 \dots f_r \in \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r = \sqrt{I}$. But then, $f \in \sqrt{I} \cap k[X_{i_1}, X_{i_2}, \dots, X_{i_d}]$ which is a contradiction. □ *End of lec. 14*

The decomposition obtained of \sqrt{I} as an intersection of finitely many primes is unique in the following sense: Call a decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r$ minimal if $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$. Suppose $\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$ 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 $\mathcal{V}(\mathfrak{q}) \subset \mathcal{V}(\sqrt{I}) = \mathcal{V}(\mathfrak{p}_1) \cup \mathcal{V}(\mathfrak{p}_2) \cup \dots \cup \mathcal{V}(\mathfrak{p}_r)$. But, $\mathcal{V}(\mathfrak{q})$ is irreducible (since \mathfrak{q} is prime), hence there exists 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 $k[X_1, \dots, X_n]$ with k algebraically closed):

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

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

◁ 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 $f \in k[X_1, X_2, \dots, X_n]$ then $U_f = k^n \setminus \mathcal{V}(f)$ is called a **basic open set**.

◁ 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.

◁ 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.

◁ 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 $k[X_1, \dots, X_n]/\sqrt{I}$, 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 $\phi : V \rightarrow W$ defined by polynomials $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ representing ϕ in the following way

$$\phi(v_1, v_2, \dots, v_n) \rightarrow (f_1(v_1, \dots, v_n), f_2(v_1, \dots, v_n), \dots, f_m(v_1, v_2, \dots, v_n))$$

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

By definition, it follows that two polynomial maps $f, g : V \rightarrow k$ 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

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

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

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

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

$$Y_i \rightarrow f_i(X_1, \dots, X_n)$$

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

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 $V \rightarrow W$ and the k -vector space of algebra homomorphisms $k[W] \rightarrow k[V]$. 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 $p : \mathbb{C}^n \rightarrow \mathbb{C}^n$ is a regular mapping given by $p = (p_1, p_2, \dots, p_n)$ with $p_i \in \mathbb{C}[X_1, \dots, X_n]$. 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. $A \simeq \mathbb{Z}[X_1, \dots, X_n]/I$. 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, 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 $A = \mathbb{Z}[x_1, \dots, x_d]$ 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}

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

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

End of lec. 15

Proof. (of the Theorem of Ax) We first prove the finite field version. Let k be a finite field, if $p : k^n \rightarrow k^n$ 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 $p_1, p_2, \dots, p_n \in k[X_1, \dots, X_n]$ be polynomials such that the regular mapping $p = (p_1, \dots, p_n) : k^n \rightarrow k^n$ is injective. Let $I \subset k[X_1, \dots, X_n, Y_1, \dots, Y_n]$ be the ideal given by

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

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 $q_{i,j} \in k[X_1, \dots, X_n, Y_1, \dots, Y_n]$ for $j = 1, \dots, n$ and $\ell_i > 0$ such that

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

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

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

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

Conversely, if Equation (2) is satisfied, over any field k , then $(a_1, \dots, a_n) \notin \text{Im}(p)$. Hence, the regular mapping $p : k^n \rightarrow k^n$ 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 $p : \mathbb{C}^n \rightarrow \mathbb{C}^n$ given by $p = (p_1, \dots, p_n)$ 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 $p : A^n \rightarrow A^n$ makes sense and the Equations (1) and (2) hold in the polynomial ring $A[X_1, \dots, X_n, Y_1, \dots, Y_n]$ and $A[X_1, \dots, X_n]$. Finally, let \mathfrak{m} be a maximal ideal in A , and consider the induced mapping

$$\bar{p} : (A/\mathfrak{m})^n \rightarrow (A/\mathfrak{m})^n$$

(which is well-defined since $\mathfrak{m} \subset A$ is an ideal). Equations (1) and (2) continue to hold over A/\mathfrak{m} hence \bar{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. \square

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

\triangleleft Find a polynomial mapping $p : \mathbb{Q}^n \rightarrow \mathbb{Q}^n$ (for any n) which is injective but not surjective. (Hint: Consider $x \rightarrow x^3$ for $x \in \mathbb{Q}$.)

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

In fact, it is also true that any polynomial mapping $p : \mathbb{R}^n \rightarrow \mathbb{R}^n$ 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 $\text{Spec}(A)$

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

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

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

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

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

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

If $A = k[X_1, X_2, \dots, X_n]$ 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 $f : A \rightarrow B$ 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

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

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

$$\mathcal{V}(I) := \{\mathfrak{p} \in \text{Spec}(A) : I \subset \mathfrak{p}\}$$

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

$$\mathcal{I}(S) := \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$$

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

► If $I_1, \dots, I_r \subset A$ are ideals, then $\mathcal{V}(I_1 \cap \dots \cap I_r) = \mathcal{V}(I_1) \cup \dots \cup \mathcal{V}(I_r)$.

► $\{I_\lambda\}_{\lambda \in \Lambda}$ is a family of ideals in A , then $\mathcal{V}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{V}(I_\lambda)$.

► $\mathcal{V}(\{0\}) = \text{Spec}(A)$ and $\mathcal{V}(A) = \emptyset$.

These properties imply that $\text{Spec}(A)$ is a topological space with closed sets given by $\mathcal{V}(I)$ for I an 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 $\mathbb{C}[M] := \{f(M) : f \in \mathbb{C}[X]\}$ where multiplication is given by matrix multiplication. Show that $\text{Spec}(\mathbb{C}[M])$ 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.)

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

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

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

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

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

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

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

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

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

Question: How can A be viewed as functions on $\text{Spec}A$?

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 $k(\mathfrak{p}) = \text{Frac}(A/\mathfrak{p})$ 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:

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

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 $\mathfrak{p} \in \mathcal{V}((f))$.

Conversely, one can characterize prime ideals in A as the kernel of homomorphisms $A \rightarrow k$ 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 $A = k[X_1, \dots, X_n]/I$ is a finitely generated k -algebra and k is algebraically closed, a maximal ideal is given by $\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ and one can canonically identify $k(\mathfrak{m}) = k[X_1, \dots, X_n]/\mathfrak{m}$ with k via the homomorphism $A \rightarrow k$ that corresponds to the evaluation homomorphism

$$A \rightarrow k \quad , \quad f \rightarrow f(a_1, a_2, \dots, a_n)$$

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 $\text{Spec}(A)$ 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.

End of lec. 16

► Let’s consider the case $A = \mathbb{Z}$. Then, $\text{Spec}(\mathbb{Z})$ 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

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

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

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

Definition 6.3. Suppose X is a topological space.

(a) We say that X is Noetherian if all the chains $Y_1 \supset Y_2 \supset \dots$ 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 $X = \text{Spec}A$ is a Noetherian topological space.

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

► If X is a Noetherian topological space, then $X = Y_1 \cup Y_2 \cup \dots \cup Y_r$ 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 $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ with $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$ such that $\sqrt{I} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_r$. Moreover, if $\mathfrak{q} \in \text{Spec}(A)$ 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

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

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

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

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

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

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

► Let $A = k[X_1, \dots, X_n]$ then we have a chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, X_2, \dots, X_n) \subsetneq A$. 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:

$R = \mathbb{Q}[X, Y, Z]$

$\dim R$

$R = \mathbb{Q}[X, Y]/(X^2, Y^3, X*Y^2)$

$\dim R$

$R = \mathbb{Z}[X]$

$\dim R$

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*

$$M_1 \subset M_2 \subset \dots \subset M$$

become stationary.

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

$$M \supset M_1 \supset M_2 \supset \dots$$

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

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

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 $(1 - ba) = 0$. \square

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.*

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

Definition 6.8. We say that 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 \mathfrak{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 $\mathfrak{m} = I$.

A chain of A -submodules $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_n = \{0\}$ 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.

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 $M = M_0 \supsetneq M_1 \supsetneq \dots \supsetneq M_p = \{0\}$ and $M = N_0 \supsetneq N_1 \supsetneq \dots \supsetneq N_q = \{0\}$ 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.

Proof. (of Theorem 6.7) We have seen that every prime ideal in an Artinian ring is maximal, so that implies $\dim A = 0$ in Proposition 6.6.

We now prove the converse. Since $\dim A = 0$ all the prime ideals are minimal (and also maximal), and since A is Noetherian, there exist finitely many of these (by the version of Corollary 4.36 for Noetherian rings), call them \mathfrak{m}_i such that $I = \sqrt{(0)} = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \dots \cap \mathfrak{m}_r$ 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, $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_r$ are pairwise coprime. By the Sunzi remainder theorem 2.3, we have that

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

Consider the chain of ideals

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

Here $I = \sqrt{(0)} = (a_1, \dots, a_n)$ for some generators by the Noetherian property. Moreover, there exists N such that $a_i^N = 0$ 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 form $M \supset M\mathfrak{m}_i$ 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. □ *End of lec. 17*

► In fact, a slightly stronger version of Theorem 6.7 is true. Namely, a ring A is Artinian if and only if A is Noetherian and $\dim A = 0$. In other words, being an Artinian ring implies that it is Noetherian. This is known as Akizuki's theorem. To show this, we need to prove that in an Artinian ring there are finitely many maximal ideals and that a power of the nilradical is zero. We can then run the above proof and see that the A admits a composition series, hence it is Noetherian. Seeing that there are finitely many maximal ideals in an Artinian ring is straightforward. Indeed, if there are infinitely many $\mathfrak{m}_1, \mathfrak{m}_2, \dots$, then the chain $\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \dots$ does not stabilize, giving a contradiction. Therefore, as in the previous proof, we have $I = \sqrt{(0)} = \mathfrak{m}_1\mathfrak{m}_2 \dots \mathfrak{m}_r$. Now, consider the chain $I \supset I^2 \supset \dots$ which, by the Artinian property, stabilises and we get $J = I^s = I^{s+i}$ for all $i \geq 0$. We want to show that J is zero. Let K be an ideal minimal among all ideals of A such that $JK \neq (0)$. Since $J^2 = J$, the set of such ideals is non-empty if $J \neq (0)$, hence a minimal element exists by the Artinian property. Let $x \in K$ such that $Jx \neq (0)$. Hence $K = (x)$ by minimality. But $J(Jx) = Jx \neq (0)$ and $Jx \subset (x)$, hence $Jx = (x)$ by minimality. This means there exists $y \in J$ such that $x = xy$. Therefore, $x = xy = xy^2 = \dots$. But, $y \in J = \sqrt{(0)}^s$ hence y is nilpotent. Therefore, $x = xy^n = 0$ for some large n , which is a contradiction. Hence, $J = (0)$ as required.

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. *Let A be a Noetherian ring with $\dim A = 0$, then A 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 $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ with $\sqrt{(0)} = \mathfrak{m}_1\mathfrak{m}_2 \dots \mathfrak{m}_r$. We also saw that there exists s such that $\sqrt{(0)}^s = (0)$. Hence, we have

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

(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

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

We leave the uniqueness statement as an exercise. □

You might have the impression that due to this theorem, we can classify all the Artinian rings. This is far from the truth. In fact, even in the case of finite-dimensional k -algebras over an algebraically closed field k , there are infinitely many isomorphism types and a pattern of classification is not known. Up to dimension 6, there are finitely many isomorphism types and a classification is known. Dimension 7 onward, there are infinitely many isomorphism types.⁶

To give you an impression of these classification results, here is a complete list (up to isomorphism) of 4-dimensional (over k) local Artinian algebras over an algebraically closed field of characteristic not equal to 2.

$$k[x]/(x^4), k[x, y]/(x^2, xy, y^3), k[x, y]/(x^2, y^2), k[x, y, z]/(x, y, z)^2$$

In characteristic 2, you have to also add $k[x, y]/(x^2 + y^2, xy)$ to the list.

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 and S is a subset of A not containing 0, we can then consider the subring

$$S^{-1}A = A[\{1/s \mid s \in S\}] \subset \text{Frac}A$$

There is the inclusion homomorphism $A \rightarrow S^{-1}A$ and every element of S becomes invertible in $S^{-1}A$. Recall that in the construction of $\text{Frac}A$ 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 $\iota : A \rightarrow B$ 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** $S^{-1}A := \{\frac{a}{s} \mid a \in A, s \in S\}$ with the following rules for addition and multiplication:

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

⁶B Poonen, Isomorphism types of commutative algebras of finite rank over an algebraically closed field.

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

$S^{-1}A$ 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 $\iota : A \rightarrow S^{-1}A$ given by $a \rightarrow \frac{a}{1}$ 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 $S^{-1}I := IS^{-1}A$ 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 $g : A \rightarrow B$ is a ring homomorphism such that $g(s)$ is invertible for all S . Then there exists a unique homomorphism $h : S^{-1}A \rightarrow B$ 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 \bar{S} be the multiplicative set given as the image of S in A/\mathfrak{n} . Observe that \bar{S} in A/\mathfrak{n} does not contain any zero divisors. Show that $\bar{S}^{-1}(A/\mathfrak{n})$ is isomorphic to $S^{-1}A$.

The following two are the main examples of localisation:

(a) Let $f \in A$ and $S := \{f^n : n = 1, 2, \dots\} \cup \{1\}$ multiplicatively closed set. Then we write $A_f := S^{-1}A$. 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 $S = \{1, X, X^2, \dots\}$. 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 $S := A \setminus \mathfrak{p}$ multiplicatively closed set. We note $A_{\mathfrak{p}} := S^{-1}A$ 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 $\iota^{-1} : \text{Spec}(S^{-1}A) \rightarrow \text{Spec}(A)$ sending is an order preserving bijection onto the subset $\{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$ with inverse given by $\mathfrak{p} \rightarrow S^{-1}\mathfrak{p}$ for $\mathfrak{p} \cap S = \emptyset$.

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

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 $abru = pustu \in \mathfrak{p}$ 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 exists $t \in S$ 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 $\{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{p} \cap S = \emptyset\}$. We will show that $\mathfrak{p} = \iota^{-1}S^{-1}\mathfrak{p}$ for all $\mathfrak{p} \in \text{Spec}(A)$ 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 exists 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 $g : A \rightarrow C$ 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 $\frac{a+I}{s+I} \in \bar{S}^{-1}(A/I)$. It is easy to check directly that this is a ring homomorphism that induces an isomorphism. \square

End of lec. 18

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

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

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 $S = A \setminus \mathfrak{p}$ for $\mathfrak{p} \in \text{Spec}(A)$ gives the following:

Corollary 6.14. If $\mathfrak{p} \subset A$ is a prime ideal and $S = A \setminus \mathfrak{p}$. Then $A_{\mathfrak{p}} := S^{-1}A$ is a local ring with the unique maximal ideal $\mathfrak{m}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$. Moreover, there is a bijection $\text{Spec}(A_{\mathfrak{p}})$ to $\{\mathfrak{q} \in \text{Spec}(A) : \mathfrak{q} \subset \mathfrak{p}\}$. 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 prime 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 $\mathfrak{p} \in \text{Spec}A$ 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 $M/\mathfrak{m}M$ 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 $x_1, \dots, x_n \in \overline{M}$ be such that $\overline{M} = Ax_1 + Ax_2 + \dots + Ax_n$ 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 $x_n \in Ax_1 + Ax_2 + \dots + Ax_{n-1}$, contradicting the minimality of n . \square

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*

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

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

Proof. Suppose $M = Ax_1 + Ax_2 + \dots + Ax_n$. Denote $\overline{x} \in M/\mathfrak{m}M$ the image of an element $x \in M$ in the quotient. Then $M/\mathfrak{m}M = \langle \overline{x}_1, \dots, \overline{x}_n \rangle_k$. Hence, $\dim_k M/\mathfrak{m}M \leq n$. Conversely, suppose $x_1, x_2, \dots, x_n \in M$ such that $\overline{x}_1, \dots, \overline{x}_n$ is a basis as a k -vector space of $M/\mathfrak{m}M$. We want to show that $Ax_1 + Ax_2 + \dots + Ax_n = M$. Let $N = Ax_1 + Ax_2 + \dots + Ax_n \subset M$. 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 $\sum_{i=1}^n a_i x_i \in N$. \square

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 $\mu(A) := \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

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's height theorem*) *Let A be a Noetherian ring. $I = (a_1, \dots, a_r)$ 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

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

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 ideals in A , however giving an upper bound from the definition is not straightforward. This is another reason why Theorem 6.17 is important.

End of lec. 19

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]), where you can also find a proof that the local ring $k[X_1, \dots, X_n]_{\mathfrak{p}}$, the localisation of $k[X_1, \dots, X_n]$ at a prime ideal \mathfrak{p} is regular. (These are applications of the homological methods in algebra which we do not get into in this course.)

The general case of Krull's height 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 / Hauptidealsatz*) *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 $S^{-1}(\mathfrak{p}) = \mathfrak{p}A_{\mathfrak{p}}$ 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 $\iota : A \rightarrow A_{\mathfrak{q}}$. 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 prime 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 $S^{-1}(\mathfrak{q})$:

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

We let $\mathfrak{q}^{(n)} = \iota^{-1}S^{-1}(\mathfrak{q}^n)$ be the 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

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

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

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

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

$$\bar{\mathfrak{p}} \supset \bar{\mathfrak{q}}^{(1)} \supset \bar{\mathfrak{q}}^{(2)} \dots$$

of ideals in \bar{A} . Because \mathfrak{p} is minimal, $\bar{\mathfrak{p}} = \mathfrak{p}/(a)$ 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 $\bar{\mathfrak{q}}^{(n)} = \bar{\mathfrak{q}}^{(n+1)}$. 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. \square

\triangleleft 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} .

\triangleleft Show that for $\mathfrak{p} = (x^4 - yz, y^2 - xz, x^3y - z^2) \subset k[x, y, z]$, $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$.

Before, we go on to give a proof of Krull's height theorem, let's already see an application of Krull's principal ideal theorem.

Theorem 6.20. *Let $\mathfrak{p} \subset \mathfrak{q}$ be prime ideals in a Noetherian ring A . If there exists a prime ideal properly between them, then there are infinitely many.*

Proof. We may pass to the integral domain A/\mathfrak{p} and suppose that $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are the only prime ideals properly between (0) and \mathfrak{q} . By prime avoidance (Proposition 2.9), we cannot have that $\mathfrak{q} \subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$. Therefore, we can pick $a \in \mathfrak{q}$ such that $a \notin \mathfrak{p}_i$ for any i . Then \mathfrak{q} is minimal over (a) , hence by Krull's principal ideal theorem $h(\mathfrak{q}) \leq 1$, which is a contradiction to the existence of at least one prime ideal between 0 and \mathfrak{q} . \square

\triangleleft Suppose A is Noetherian, and $\sqrt{(0)} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_s$ 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 not a zero-divisor. *End of lec. 20*

Let us now turn to the proof of Krull's height theorem.

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 $I = (a_1, \dots, a_r)$.

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 since $h(\mathfrak{p}_1) = h(\mathfrak{p}) - 1$.

We have $\sqrt{J} = \mathfrak{p}$. To see this, note that since A is Noetherian, we can write $\sqrt{J} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ 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 $i = 2, \dots, r$ 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 $I_1 := (y_2, \dots, y_r)$. We claim that \mathfrak{p}_1 is minimal among prime ideals containing I_1 . Indeed, consider the quotient map $\pi : A \rightarrow A/I_1$. Write $\pi(a) = \bar{a}$. We have $(0) \neq (\bar{a}_1) \subset \bar{\mathfrak{p}} \subset A/I_1$. We claim that $\bar{\mathfrak{p}}$ is minimal in A/I_1 with $(\bar{a}_1) \subset \bar{\mathfrak{p}}$. It suffices to show that $\sqrt{(\bar{a}_1)} = \bar{\mathfrak{p}}$. To see this, first observe that

$$(a_1, y_2, \dots, y_r) = (a_1, a_2^N - a_1 x_2, a_3^N - a_1 x_3, \dots, a_r^N - a_1 x_r) = (a_1, a_2^N, a_3^N, \dots, a_r^N)$$

On the other hand, we have $I = (a_1, \dots, a_r) \subset \mathfrak{p}$ 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, $x^{srN} \in (a_1^N, a_2^N, \dots, a_r^N) \subset (a_1, y_2, \dots, y_r)$. It follows that $\sqrt{(a_1, y_2, \dots, y_r)} = \mathfrak{p}$. This, in turn, implies that $\sqrt{(\bar{a}_1)} = \bar{\mathfrak{p}}$. Finally, by the Hauptidealsatz, we have $h(\bar{\mathfrak{p}}) \leq 1$. Hence $h(\bar{\mathfrak{p}}) = 0$ which in turn implies that \mathfrak{p}_1 is minimal prime ideal containing I_1 , as required. \square

Corollary 6.21. *A local Noetherian ring has finite dimension.*

Proof. By Krull's height theorem $\dim(A) \leq \mu(A)$ and $\mu(A)$ is finite. \square

Somewhat disturbingly, a Noetherian ring does not have to have finite dimension.

\triangleleft (Nagata) Consider the ring $A = k[x_1, x_2, x_3, \dots]$ (polynomial ring in infinitely many variables). For $i = 1, 2, \dots$, let m_i be an increasing sequence of integers such that $\lim_{i \rightarrow \infty} m_{i+1} - m_i = \infty$ (for example, take $m_i = 2^i$). Let $\mathfrak{p}_i = (x_{m_i+1}, x_{m_i+2}, \dots, x_{m_{i+1}})$. We set $S = A \setminus \cup_i \mathfrak{p}_i$, and consider the ring $R = S^{-1}A$. Then, show that R is a Noetherian ring, the maximal ideals of R are precisely $\mathfrak{m}_i = S^{-1}\mathfrak{p}_i$ with $h(\mathfrak{m}_i) = m_{i+1} - m_i$, thus $\lim_{i \rightarrow \infty} h(\mathfrak{m}_i) = \infty$.

Corollary 6.22. *Let k be an algebraically closed field, $\dim k[X_1, X_2, \dots, X_n] = n$.*

Proof. Let $A = k[X_1, X_2, \dots, X_n]$. We have already seen that $\dim A \geq n$ because of the existence of the chain of prime ideals $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \dots \subsetneq (X_1, \dots, X_n) \subsetneq A$. Let $(0) \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_r \subsetneq A$ be a chain of prime ideal with \mathfrak{p}_r a maximal ideal. By Hilbert's Nullstellensatz, we know that $\mathfrak{p}_r = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ with $a_i \in k$. By Krull's height theorem, we see that $h(\mathfrak{p}_r) \leq n$. It follows that $\dim k[X_1, X_2, \dots, X_n] = n$. \square

In Corollary 6.22, the assumption that k is algebraically closed can be dropped. To adapt the given proof, we need the following generalisation of (weak) Nullstellensatz.

Theorem 6.23. *(weak Nullstellensatz for arbitrary field) Let k be an arbitrary field. Every maximal ideal $\mathfrak{m} \subset k[X_1, \dots, X_n]$ is of the form*

$$\mathfrak{m} = (f_1, f_2, \dots, f_n) \text{ with } f_i \in k[X_1, \dots, X_i] = k[X_1, \dots, X_{i-1}][X_i] \text{ monic in } X_i.$$

Proof. By Zariski's lemma, we know that the field $k[X_1, \dots, X_n]/\mathfrak{m}$ is an algebraic extension of k . Write $k(\alpha_1, \dots, \alpha_n)$ for this algebraic extension where $\alpha_i = X_i + \mathfrak{m}$. Let $f_1 \in k[X_1] \cap \mathfrak{m}$ be the minimal polynomial of α_1 over k . Then, $(f_1) \subset k[X_1]$ is a maximal ideal, and $k[X_1]/(f_1) = k[\alpha_1]$ is a field isomorphic to $k(\alpha_1)$. Now, since $k(\alpha_1) = k[\alpha_1]$, the minimal polynomial of α_2 over $k(\alpha_1)$ is a monic polynomial in $k[\alpha_1][X_2]$, hence we can find a polynomial $f_2 \in k[X_1, X_2] \cap \mathfrak{m}$ monic in X_2 with $f_2(\alpha_1, X_2)$ is the minimal polynomial of α_2 over $k(\alpha_1)$. In a similar fashion, for all i , we can find a polynomial $f_i \in k[X_1, \dots, X_i] \cap \mathfrak{m}$ monic in X_i such that $f_i(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, X_i)$ is the minimal polynomial of α_i over $k(\alpha_1, \dots, \alpha_{i-1})$.

We next want to show that the kernel of the map $\phi : k[X_1, X_2, \dots, X_n] \rightarrow k(\alpha_1, \dots, \alpha_n)$ sending $X_i \rightarrow \alpha_i$ is $\mathfrak{m} = (f_1, \dots, f_n)$. Note that by construction $f_i \in \mathfrak{m}$. Let $p \in k[X_1, \dots, X_n]$ such that $\phi(p) = 0$, that is $p(\alpha_1, \dots, \alpha_n) = 0$. In particular, $p(\alpha_1, \dots, \alpha_{n-1}, X_n)$ is divisible by $f_n(\alpha_1, \dots, \alpha_{n-1}, X_n)$. Considering $p, f_n \in k[X_1, \dots, X_{n-1}][X_n]$ with f_n monic in X_n , we can divide p by f_n and write $p = q_n f_n + r_n$ for some $q_n, r_n \in k[X_1, \dots, X_n]$ with $r_n(\alpha_1, \dots, \alpha_{n-1}, X_n) = 0$ since $f_n(\alpha_1, \dots, \alpha_{n-1}, X_n)$ is the minimal polynomial of α_n over $k(\alpha_1, \dots, \alpha_{n-1})$. Similarly, considering r_n as a polynomial in $k[X_1, \dots, X_{n-2}, X_n][X_{n-1}]$ and $f_{n-1} \in k[X_1, \dots, X_{n-2}][X_{n-1}]$

with f_{n-1} monic in X_{n-1} , we can write $r_n = q_{n-1}f_{n-1} + r_{n-1}$ with $r_{n-1}(\alpha_1, \dots, \alpha_{n-2}, X_{n-1}, X_n) = 0$. Proceeding this way, we get

$$p = q_1f_1 + q_2f_2 + \dots + q_nf_n + r$$

with $r(X_1, X_2, \dots, X_n) = 0$, that is, $r = 0$. Thus, $p \in (f_1, \dots, f_n)$. \square

Corollary 6.24. *For any field k , $\dim k[X_1, \dots, X_n] = n$.*

Proof. The proof is essentially identical to the proof of Corollary 6.22 using the generators f_1, f_2, \dots, f_n from Theorem 6.23 of any maximal ideal. \square *End of lec. 21*

We let $V \subset k^n$ be an irreducible affine variety and $I(V) \subset k[X_1, X_2, \dots, X_n]$ is the corresponding prime ideal. The ring of regular functions on V is $A = k[X_1, X_2, \dots, X_n]/I(V)$. In this setting, we defined $\dim V := \deg HP_{I(V)}(t)$. On the other hand, one may ask how does this compare to $\dim A$?

Theorem 6.25. $\dim V = \dim A$.

To see this, first, by the Noether normalisation theorem, we know that there exist algebraically independent elements a_1, a_2, \dots, a_d such that $A \supset k[a_1, a_2, \dots, a_d]$ is integral. Moreover, by Proposition 4.26, we have $d = \dim V$. The Corollary 6.24 showed that $\dim k[a_1, a_2, \dots, a_d] = d$. Finally, to conclude that $\dim V = \dim A$, we need the following theorem.

Theorem 6.26. (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 $\text{Spec} B \rightarrow \text{Spec} A$ is surjective.*

(2) (Incomparability) *If $\mathfrak{q}_1, \mathfrak{q}_2 \subset B$ are two prime ideals such that $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$ and $\mathfrak{q}_1 \subset \mathfrak{q}_2$ then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

(3) (Going up) *Given prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset A$ and a prime ideal $\mathfrak{q}_0 \subset B$ such that $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$, there exists a prime ideal $\mathfrak{q}_1 \subset B$ such that $\mathfrak{q}_0 \subset \mathfrak{q}_1$ and $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.*

As a consequence of (1), (2) and (3), we have $\dim A = \dim B$.

We will need the following lemma in the proof:

Lemma 6.27. *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 $a_0, a_1, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

- (i) Apply the homomorphism $- : B \rightarrow B/I$, 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

$$\frac{b^n}{s^n} + \frac{a_{n-1} b^{n-1}}{s} + \dots + \frac{a_1 b}{s^{n-1}} + \frac{a_0}{s^n} = 0$$

from which we see that b/s is integral over $S^{-1}A$. \square

Lemma 6.28. *If B is integral over A , then the canonical map $\text{Spec}B \rightarrow \text{Spec}A$ sends maximal ideals to maximal ideals.*

Proof. Let $\mathfrak{m} \subset B$ be a maximal ideal, and let $\mathfrak{n} = \mathfrak{m} \cap A$. Then by Lemma 6.27 (i), we get that the field B/\mathfrak{m} is integral over A/\mathfrak{n} , hence by Lemma 4.22(d) A/\mathfrak{n} is also a field, which means \mathfrak{n} is a maximal ideal. \square

Proof. (of Cohen-Seidenberg) Let $S = A \setminus \mathfrak{p}$ be the multiplicatively closed set. By Lemma 6.27 the local ring $S^{-1}B$ is an integral extension of the local ring $S^{-1}A$. From the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow \alpha & & \downarrow \beta \\ S^{-1}A & \longrightarrow & S^{-1}B \end{array}$$

and using Lemma 6.28, we see that 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 $A_{\mathfrak{p}}$. Now, let $\mathfrak{m} \subset S^{-1}B$ be a maximal ideal, then $\mathfrak{m} \cap S^{-1}A$ is a maximal ideal in $S^{-1}A$ hence is the unique maximal ideal $S^{-1}\mathfrak{p}$. Then, $\beta^{-1}(\mathfrak{m})$ is a prime ideal lying over \mathfrak{p} . This proves (1).

Next, suppose \mathfrak{q}_1 and \mathfrak{q}_2 are prime ideals in B with $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}$ with $\mathfrak{q}_1 \subset \mathfrak{q}_2$, then $S^{-1}\mathfrak{q}_1$ and $S^{-1}\mathfrak{q}_2$ are maximal ideals in $S^{-1}B$ lying over the maximal ideal $S^{-1}\mathfrak{p} \subset A_{\mathfrak{p}}$, and $S^{-1}\mathfrak{q}_1 \subset S^{-1}\mathfrak{q}_2$. Hence, it follows that $S^{-1}\mathfrak{q}_1 = S^{-1}\mathfrak{q}_2$ and therefore, $\mathfrak{q}_1 = \mathfrak{q}_2$. This proves (2).

We next turn to the proof of (3) and $\dim A \leq \dim B$ at the same time. Suppose that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n \subsetneq A$ 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, $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_i$ 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 6.27 (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 $\mathfrak{q}_{i+1} \cap A = \mathfrak{p}_{i+1}$.

Finally, suppose $\mathfrak{q}_0 \subsetneq \dots \subsetneq \mathfrak{q}_n \subsetneq B$ is a chain of prime ideals. Then $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ and the corresponding chain $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n \subsetneq A$ has the same length by part (2). Thus, it follows that $\dim B \leq \dim A$. Hence, we conclude that $\dim A = \dim B$ as required. \square

\triangleleft Let A be a subring of B (not necessarily an integral extension). Show that if the going-up property holds for the ring extension $A \subset B$, then lying-over property also holds.

End of lec. 22

6.5 Valuation rings

Throughout the course, we have developed the notion of dimension, first in the case of polynomial rings $k[X_1, \dots, X_n]$ via the Hilbert polynomial and then in general for arbitrary rings via Krull dimension. We understood that 0-dimensional Noetherian rings are precisely Artinian rings. We next want to explore the structure of 1-dimensional Noetherian rings.

Definition 6.29. *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

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

Thus $\mathbb{Z}_{(p)}$ 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,

$$R_{(\pi)} := \left\{ \frac{a}{b} : a, b \in R, \pi \nmid b \right\}$$

is a valuation ring.

► $k[[X]]$ is a valuation ring. Its field of fractions is given by the formal Laurent series $k((X)) := k[[X]][X^{-1}]$.

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 6.30. *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, $\mathfrak{m}_R := \{x \in R : x \text{ non-unit}\}$ 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, $x \notin R$. \square

< Prove that in a valuation ring, any radical ideal is prime.

< Suppose R is a valuation ring with field of fractions K . Show that any subring R' of K with $R \subset R' \subset K$ is isomorphic to $R_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R$. (Hint: Consider $\mathfrak{p} = \mathfrak{m}' \cap R$, where $\mathfrak{m}' \subset R'$ is the maximal ideal of R' .)

Let $A \subset R$ be rings, we say that an ideal $I \subset A$ **survives in R** if $IR \neq R$, or equivalently $1 \notin IR$.

Lemma 6.31. *Let $R \subset K$ be a subring of a field K , and $0 \neq x \in K$, I a proper ideal in R . Then, I survives either in $R[x]$ or $R[x^{-1}]$.*

Proof. Suppose the conclusion fails, then we have equations

$$1 = a_0 + a_1x + \dots + a_nx^n \text{ with } a_i \in I$$

$$1 = b_0 + b_1x^{-1} + \dots + b_mx^{-m} \text{ with } b_i \in I$$

By symmetry, we may assume that $n \geq m$ and we choose n as small as possible. Multiplying the first equation by $(1 - b_0)$ we get

$$1 = b_0 + a_0(1 - b_0) + a_1(1 - b_0)x + \dots + a_n(1 - b_0)x^n$$

Multiplying the second equation with x^n we get

$$(1 - b_0)x^n = b_1x^{n-1} + \dots + b_mx^{n-m} \text{ with } b_i \in I$$

Using this to substitute for $(1 - b_0)x^n$ in the equation before, we arrive at

$$1 = b_0 + (1 - b_0)a_0 + (1 - b_0)a_1x + \dots + a_n(b_1x^{n-1} + \dots + b_mx^{n-m})$$

which gives an equation of degree less than n with each coefficient in I , a contradiction. \square

Theorem 6.32. *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 $\mathfrak{m}_{\mathfrak{p}} = S^{-1}\mathfrak{p}$ where $S = A \setminus \mathfrak{p}$. Therefore, without loss of generality, we assume that A itself is a local ring and \mathfrak{p} is its maximal ideal.

Let us define

$$\mathcal{F} := \{B \subset K : B \text{ subring, } A \subset B \text{ and } \mathfrak{p} \text{ survives in } B\}$$

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 $x^{-1} \in R$. Consider $R \subsetneq R[x] \subset K$. By the maximality of R , we have $R[x] \notin \mathcal{F}$. Hence, by Lemma 6.31, it must be that \mathfrak{p} survives in $R[x^{-1}]$ but then by maximal of R , we conclude that $R = R[x^{-1}]$, hence $x^{-1} \in R$. \square

Theorem 6.33. *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

$$x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0 = 0.$$

Since R is a valuation ring and $x \in K \setminus R$, we have $x^{-1} \in \mathfrak{m}_R$. Thus, we get

$$1 + a_{m-1}x^{-1} + \dots + a_1x^{1-m} + a_0x^{-m} = 0$$

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

$$1 = a_1x^{-1} + \dots + a_nx^{-n} \text{ with } a_i \in A$$

Multiplying with x^n gives

$$x^n = a_1x^{n-1} + \dots + a_n$$

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 6.32, there exist a valuation ring $R \subset K$ with $A[x^{-1}] \subset R$ and $\mathfrak{m}_R \cap A[x^{-1}] = \mathfrak{m}$. Therefore, $x^{-1} \in \mathfrak{m}_R$. Hence, $x \in K \setminus R$ as desired. \square

End of lec. 23

\triangleleft Show that if A is normal, then $A[X]$ is also normal. (Hint: Use Theorem 6.33 to reduce to the case where A is a valuation ring.)

You may wonder why are the valuation rings are called valuation rings. What are the “valuations” on them?

Definition 6.34. An **ordered abelian 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.

► An ordered abelian group is torsion free.

Definition 6.35. Let K be a field and Γ an ordered abelian group. A map $\nu : K \rightarrow \Gamma \cup \{\infty\}$ 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 $x = 0$.

► 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. It also follows that $\nu(x) = 0$ implies that $x \in R$ is a unit.

Proposition 6.36. Let $R \subset K$ be a valuation ring, then there exists an ordered group Γ and a valuation $\nu : K \rightarrow \Gamma \cup \{\infty\}$ such that $R = R_\nu$.

Proof. Given a valuation ring $R \subset K$, let us define the abelian group

$$\Gamma := \{xR : x \in K \setminus \{0\}\}$$

with addition $xR + yR = xyR$ and additive identity 0 is represented by $1 \cdot R$. In a similar way to the argument giving Proposition 6.30(i) we can prove that one has either $xR \subset yR$ or $yR \subset xR$. We define a total order on Γ by setting $xR \leq yR$ if and only if $yR \subset xR$ (opposite of the inclusion order). We can then define a valuation $\nu : K \rightarrow \Gamma \cup \{\infty\}$ by setting $\nu(x) = xR$. It is then easy to verify that $R = R_\nu$ and $\mathfrak{m}_R = \mathfrak{m}_\nu$. \square

We next want to understand valuation rings that are Noetherian.

Theorem 6.37. Let R be a valuation ring in K and $R \neq K$. Then, the following are equivalent:

(1) R is a **discrete valuation ring (DVR)**, that is, there exists a surjective valuation $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ such that $R_\nu = R$,

(2) R is a *principal ideal domain*,

(3) R is *Noetherian*.

Proof. (1) \implies (2) Let $t \in K$ such that $\nu(t) = 1$. We claim that $\mathfrak{m}_R = (t)$. Indeed, let $x \in \mathfrak{m}_R$, then $\nu(x) = n > 0$. So, $\nu(xt^{-n}) = \nu(x) + \nu(t^{-n}) = \nu(x) - n\nu(t) = 0$. Hence, $x = ut^n$ for some unit $u \in R$. Thus, $\mathfrak{m}_R = (t)$. Now, let I be an arbitrary ideal in R . Let $m = \min\{\nu(a) : 0 \neq a \in I\} \in \mathbb{Z}_{\geq 0}$. Take $a \in I$, such that $\nu(a) = m$. If $m = 0$, then a is a unit, hence $I = R = (1)$ principal. If $m > 0$, then as before $a = ut^m$ with u a unit, and so $(a) = (t^m)$. We claim that $I = (t^m)$. Indeed, if $0 \neq b \in I$, then $\nu(b) \geq m$ so $\nu(bt^{-m}) \geq 0$, hence $b \in Rt^m$.

(2) \implies (3) is trivial.

(3) \implies (2) Let $I \in R$ be an ideal. Since R is Noetherian, $I = Rv_1 + Rv_2 + \dots + Rv_n$ with $v_i \in I$. Choose the notation so that $Rv_1 \subset Rv_2 \subset \dots \subset Rv_n$. Then $I = Rv_n$ is principal.

(2) \implies (1) We have $\mathfrak{m}_R = (t)$ for some $t \in R$. Let $I := \bigcap_{n=1}^{\infty} (t^n) \subset R$. We claim that $I = (0)$. Indeed, since R is principal $I = (a)$ for some $a \in R$. Since $I \subset \mathfrak{m}_R$, we have $a = zt$ with $z \in R$. Now, for all $n \geq 1$, $a \in (t^n)$, so $a = ct^n$ with $c \in R$. So, $z = ct^{n-1} \in (t^{n-1})$ hence $z \in I$. Thus, $z = ra$ with $r \in R$. So, $a = rat$, thus $a(1 - rt) = 0$ but since $rt \in \mathfrak{m}_r$, $1 - rt$ is invertible, hence $a = 0$. Now, consider the chain of ideals

$$(t) \supsetneq (t^2) \supsetneq \dots$$

Given $x \in R$, since $\bigcap_{n=1}^{\infty} (t^n) = 0$, there exists $n \geq 0$ such that $x \in (t^n) \setminus (t^{n+1})$, and we define $\nu(x) = n$. It is easy to see that if $\frac{a}{b} = \frac{c}{d} \in K$, one has $\nu(a) - \nu(b) = \nu(c) - \nu(d)$. Thus, we define the valuation $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ by letting $\nu(\frac{a}{b}) = \nu(a) - \nu(b)$ for $a, b \in R$. We leave it as an exercise to verify that ν is indeed a valuation. \square

► During the course of the proof, we have shown that if R is a valuation ring that satisfies any of the three equivalent conditions then all the ideals in R are of the form (t^n) for some $n \geq 0$ and any $t \in R$ with $\nu(t) = 1$.

► $\mathbb{Z}_{(p)}$ is a DVR with (p) as maximal ideal. $\nu : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$ is given by $\nu(\frac{a}{b}) = \nu(p^n \frac{a'}{b'}) = n$ if $p \nmid a'$ and $p \nmid b'$.

► $k[X]_{(X)} = \{\frac{f(X)}{g(X)} : f(X), g(X) \in k[X], g(0) \neq 0\}$ is a DVR with maximal ideal (X) . $\nu : k(X) \rightarrow \mathbb{Z} \cup \{\infty\}$ is given by $\nu(\frac{f}{g}) = \nu(X^n \frac{\bar{f}}{\bar{g}}) = n$ if $X \nmid \bar{f}$ and $X \nmid \bar{g}$.

► Consider the **field of Puiseux series**

$$K = \bigcup_{n \geq 1} k\left(\left(t^{\frac{1}{n}}\right)\right) = \left\{ \sum_{i \geq m} a_i t^{\frac{i}{n}} : a_i \in k, m \in \mathbb{Z}, n \in \mathbb{Z}_{>0} \right\}$$

is the union (over n) of formal Laurent series in $t^{\frac{1}{n}}$. It admits a valuation $\nu : K \rightarrow \mathbb{Q} \cup \{\infty\}$ sending an element to the smallest power of t such that the coefficient is non-zero. The valuation ring is

$$R = \bigcup_{n \geq 1} k\left[\left[t^{\frac{1}{n}}\right]\right].$$

< Show that $(t^{1/2^n})$ is an ascending chain of ideals in R , hence R is not Noetherian.

Finally, we come to the main theorem on discrete valuation rings.

Theorem 6.38. *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 $\dim R = 1$.

End of lec. 24

For the proof, we have to develop a few tools.

Definition 6.39. Let A be a commutative ring. A **multiplicative \mathbb{N} -filtration** of A is a sequence of subgroups $\mathcal{F} = \{A_n\}_{n \in \mathbb{N}}$ of the additive group of A , such that $A_m A_n \subset A_{m+n}$ for all $m, n \geq 0$.

The main example of an \mathbb{N} -filtration on a ring is given by the I -adic filtration associated to an ideal $I \subset A$. This is defined by setting $A_n = I^n$ for $n \geq 0$. In particular, this means $A_0 = A$.

Definition 6.40. Given an \mathbb{N} -filtration $\mathcal{F} = \{A_n\}_{n \in \mathbb{N}}$ on a ring A , the subring of $A[T]$

$$R(\mathcal{F}) := \bigoplus_{n \geq 0} A_n T^n \subset A[T]$$

is called the **Rees algebra**.

Note that A_0 is a subring of $R(\mathcal{F})$ hence $R(\mathcal{F})$ is an A_0 -algebra.

We shall be concerned with the special case when \mathcal{F} is an I -adic filtration. Then, $R(\mathcal{F})$ is an A -algebra, and we write it as

$$B_I A := A \oplus I \oplus I^2 \oplus \dots$$

and refer to it as the **blow-up algebra** of I in A .

Definition 6.41. Let A be a ring and $I \subset A$ is an ideal. An **I -filtration** of an A -module M is an infinite descending chain:

$$M = M_0 \supset M_1 \supset \dots \supset M_n \supset \dots$$

of A -submodules of M such that $IM_n \subset M_{n+1}$ for all $n \geq 0$. We say that an I -filtration is **I -stable** if $IM_n = M_{n+1}$ for all sufficiently large n .

If M is an A -module with an I -adic filtration, then the direct sum

$$B_I M = M_0 \oplus M_1 \oplus \dots$$

becomes a module over $B_I A$.

Proposition 6.42. Let A be a Noetherian ring, let $I \subset A$ an ideal, let M be a finitely generated A -module, and let $(M_n)_{n \geq 0}$ be an I -filtration of M . Then the following are equivalent:

- (i) $B_I M$ is a finitely generated $B_I A$ -module,
- (ii) the I -filtration $(M_n)_{n \geq 0}$ is I -stable.

Proof. As A is Noetherian and the ideal I is finitely generated, $B_I A$ is finitely generated as an A -algebra, so it is Noetherian by Hilbert's basis theorem. Since A is Noetherian and M is finitely generated, we get that M is Noetherian. Therefore, M_n is finitely generated for each n .

Hence so is each $Q_n = \bigoplus_{r=0}^n M_r$. This is a subgroup of $B_I M$ but may not be an $B_I A$ -module in general, however it gives the following finitely generated $B_I A$ -module

$$B_I^n M = M_0 \oplus \dots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \dots$$

The modules $B_I^n M$ form an ascending chain whose union is $B_I M$. Since $B_I A$ is Noetherian, we get that $B_I M$ is finitely generated $B_I A$ -module if and only if $B_I M$ is Noetherian if and only if the chain $B_I^n M$ stabilizes if and only if $(M_n)_{n \geq 0}$ is I -stable. \square

Lemma 6.43. (*Artin-Rees*) *Let A be a Noetherian ring. M be a finitely generated A -module, $N \subset M$ a submodule, and $I \subset A$ is an ideal. Then there exists $c > 0$ such that*

$$I^n M \cap N = I^{n-c}(I^c M \cap N) \text{ for all } n > c.$$

Proof. We have an I -filtration on M given by

$$M \supset IM \supset I^2 M \supset \dots$$

which is I -stable and gives a finitely generated $B_I A$ module $B_I M$. Now, we have $I(I^n M \cap N) \subset (I^{n+1} M \cap IN) \subset I^{n+1} M \cap N$ so $(I^n M \cap N)_{n \geq 0}$ is an I -filtration. Hence it defines a $B_I A$ -module which is a submodule of $B_I M$ and therefore finitely generated since $B_I A$ is Noetherian. Thus, the result follow from Propostion 6.42. \square

Corollary 6.44. (*Krull's intersection theorem*) *Let A be a local Noetherian ring with maximal ideal \mathfrak{m} . Let M be a finitely generated A -module, then*

$$\bigcap_{n > 0} \mathfrak{m}^n M = \{0\}$$

In particular, for $M = A$, we have $\bigcap_{n > 0} \mathfrak{m}^n = \{0\}$.

Proof. Let N be the finitely generated A -module given by $N := \bigcap_{n > 0} \mathfrak{m}^n M$. By Nakayama's lemma, it suffices to show that $\mathfrak{m}N = N$. By Artin-Rees lemma, there exists $c > 0$ such that $N = \mathfrak{m}^n M \cap N = \mathfrak{m}^{n-c}(\mathfrak{m}^c M \cap N) = \mathfrak{m}^{n-c}N \subset \mathfrak{m}N$. Thus, it follows that $N = 0$. \square

We are now ready to prove the main theorem on discrete valuation rings.

Proof. (of Theorem 6.38) (1) \implies (2) follows from Theorem 6.37. (2) \implies (3) is trivial. We now prove (3) \implies (1). Suppose R is Noetherian, local, $\dim R > 0$ and maximal ideal $\mathfrak{m} = (t)$ for $t \in R$. Then, for all n , we must have $\mathfrak{m}^n \neq (0)$. Indeed, otherwise, if $\mathfrak{m}^n = (0)$, then $\mathfrak{m} = \sqrt{(0)}$. So, this would give \mathfrak{m} is the unique prime ideal of R , which implies $\dim R = 0$, a contradiction.

Now, by Krull's intersection theorem, we have $\bigcap_{n > 0} \mathfrak{m}^n = 0$. Therefore, for all $y \in R$, there exists an $n \geq 0$ such that $y \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. But $\mathfrak{m}^n = (t^n)$, hence $y = ut^n$ for some unit u . (If u is not a unit, then $u \in (t)$, so $y \in \mathfrak{m}^{n+1}$, a contradiction). This implies that R is an integral

domain: $0 \neq y = ut^n$ and $0 \neq z = vt^m$ with $n, m \geq 0$ and u, v units, we get $yz = uvt^{n+m} \neq 0$. Then, the field of fractions is $K = \{ut^n : u \text{ unit in } R, n \in \mathbb{Z}\} \cup \{0\}$ and the valuation is given by $\nu(ut^n) = n$.

Next, we prove (1) \implies (4). R is a discrete valuation ring hence $\mathfrak{m} = (t)$ and

$$R \supset (t) \supset (t^2) \supset \dots \supset (0)$$

are all the ideals in R . The only prime ideals are (t) and (0) . Hence $\dim R = 1$. As R is principal, it is Noetherian. Finally, R is a valuation ring, hence it is normal.

Finally, we prove (4) \implies (3). Thus, we suppose R is a Noetherian, local, normal and $\dim R = 1$ and we want to show that the maximal ideal \mathfrak{m} of R is principal.

Since R is Noetherian, by Nakayama's lemma if $\mathfrak{m}^2 = \mathfrak{m}$, then $\mathfrak{m} = 0$. Hence, $\mathfrak{m}^2 \neq \mathfrak{m}$. Let $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. We want to show that $\mathfrak{m} = (t)$.

Suppose $\mathfrak{m} \neq (t)$, so \mathfrak{m} contains an element $a \notin (t)$. Consider the ideal $I_a = ((t) : (a)) = \{x \in R : xa \in (t)\}$. Since $a \notin (t)$, we have I_a is proper. Note that $t \in I_a$ so $I_a \neq 0$. As R is Noetherian, the family of ideals $\{I_a : a \in \mathfrak{m} \setminus (t)\}$ has a maximal element with respect to inclusion, so let us call I_a the maximal element.

Claim: I_a is prime: Suppose $x, y \in R$ such that $xy \in I_a$ then $xya \in (t)$. Suppose that $x \notin I_a$ then $xa \notin (t)$, then $I_a \subset I_{xa} \subsetneq R$. By maximality of I_a , it follows that $I_a = I_{xa}$, and $y \in I_{xa}$ gives $y \in I_a$. Thus, I_a is prime, and as the dimension of R is one, it must be that $I_a = \mathfrak{m}$.

Let $K = \text{Frac}R$. Then, $a/t \in K$.

Claims: (i) $a/t \notin R$ and (ii) $(a/t)\mathfrak{m} \subset R$ is a proper ideal.

Proof of (i): If $a/t \in R$, then $a = (a/t)t \in (t)$ but this contradicts the choice of a .

Proof of (ii): Since $\mathfrak{m} = I_a$, if $x \in \mathfrak{m}$, then $ax \in (t)$, so $(a/t)x = t^{-1}ax \in R$. We conclude that $(a/t)\mathfrak{m} \subset R$ is an ideal. In fact, this is a proper ideal. Otherwise, $t = ab$ for some $b \in \mathfrak{m}$. But then, $t \in \mathfrak{m}^2$ which is false.

Since R is a local, we have $(a/t)\mathfrak{m} \subset \mathfrak{m}$. Since R is Noetherian, we have $\mathfrak{m} = (a_1, \dots, a_r)$ for some r with $a_i \in R$. Now, $(a/t)\mathfrak{m} \subset \mathfrak{m}$ implies that we can write

$$(a/t)a_j = \sum_{i=1}^r c_{ij}a_i \text{ with } c_{ij} \in R$$

As before, by Cramer's rule we deduce

$$a_i \det(N - (a/t)I_r) = 0 \text{ for all } i = 1, \dots, r$$

where N is the r -by- r matrix with entries c_{ij} . Since R is an integral domain, we conclude that $\det(N - (a/t)I_r) = 0$, hence this implies that (a/t) is integral over R . But R is normal, hence $a/t \in R$, a contradiction. Hence $\mathfrak{m} = (t)$ as required. \square *End of lec. 25*

Proposition 6.45. *Let A be an integral domain, then A is normal if and only if $A_{\mathfrak{p}}$ is normal for all prime ideals \mathfrak{p} .*

Proof. Suppose A is normal, let $K = \text{Frac}(A)$, and let S be any multiplicative set. If $x \in K$ is integral over $S^{-1}A$, then we have an equation

$$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$$

with $b_i = a_i/s_i \in S^{-1}A$. Multiplying this equation with s^n for $s = s_0s_1 \dots s_{n-1}$ shows that sx is integral over A , hence $sx \in A$ which gives $x \in S^{-1}A$.

Conversely, suppose $A_{\mathfrak{p}}$ is normal for all prime \mathfrak{p} . The normality of A follows from the following claim: $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$ where intersection is over all prime ideals. For if $x \in K$ is integral over A , then it is integral over all $A_{\mathfrak{p}}$ and if the latter are integrally closed, $x \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$.

To prove the claim, note that it suffices to show that $A = \bigcap_{\mathfrak{m}} A_{\mathfrak{m}}$ where intersection is over all maximal ideals. Let $x \in K$, and consider the ideal $I_x = \{a \in A : ax \in A\}$ - the ideal of denominators of x . Now $x \notin A_{\mathfrak{m}}$ if and only if $I_x \subset \mathfrak{m}$. Thus, if $x \in A_{\mathfrak{m}}$ for all \mathfrak{m} , then $1 \in I_x$, hence $x \in A$, as required. \square

For example, let $K \supset \mathbb{Q}$ be a number field, that is an algebraic field extension of \mathbb{Q} , and let $\mathcal{O}_K = \overline{\mathbb{Z}}_K$ the integral closure of \mathbb{Z} in K . This is a Noetherian ring and all the non-zero prime ideals are maximal, hence $\dim \mathcal{O}_K = 1$. Now let \mathfrak{p} be a prime ideal in \mathcal{O}_K and consider the ring $\mathcal{O}_{K,\mathfrak{p}} = \{a/b \in K : a \in \mathcal{O}_K, b \notin \mathfrak{p}\}$. This is a local, Noetherian, normal ring of dimension 1. Hence, by Theorem 6.38, it is a DVR.

Definition 6.46. *For an integral domain R with field of fractions K , a **fractional ideal** of R is an R -submodule I in K such that $I \neq 0$ and there exists a non-zero element $a \in R$ such that $aI \subset R$.*

In particular, ordinary ideals are fractional (just take $a=1$). The element a can be thought as clearing out denominators in I . Every finitely generated R -submodule I in K is a fractional ideal; for if I is generated by $x_1, \dots, x_n \in K$, we can write $x_i = y_i/a$ for $y_i \in R$ and $a \in R$, hence $aI \subset R$. Conversely, since as an R -module, aI is isomorphic to I , if R is Noetherian any fractional ideal is finitely generated. For a fractional ideal I , we define $I^{-1} = \{b \in K : bI \subset R\}$. The fractional ideal I is said to be **invertible** if $II^{-1} = R$. More explicitly, this means that there exist finitely many elements $a_i \in I$ and $b_i \in I^{-1}$ such that $\sum a_i b_i = 1$.

Every non-zero principal fractional ideal (a) , for $a \in K$, is invertible, its inverse being (a^{-1}) .

Lemma 6.47. *If R is a local, integral domain, then every invertible ideal is principal.*

Proof. Let $a_i \in I, b_i \in I^{-1}$ such that $\sum a_i b_i = 1$, then at least one of the $a_i b_i$ must be a unit. Say, $a_1 b_1$ is a unit, then $I = (a_1)$. Indeed, let $a_1 b_1 u = 1$ then for any $x \in I$, $x = a_1 (b_1 u x) \in (a_1)$ since $b_1 u x \in R$ as $u x \in I$ and $b_1 \in I^{-1}$. \square

◁ Suppose $I \subset R$ is invertible, and S a multiplicative set, the $S^{-1}I$ is invertible in $S^{-1}R$.

An integral domain for which every non-zero ideal is invertible is called a **Dedekind domain**. The ring of integers \mathcal{O}_K are Dedekind domains. This follows from the following characterisation of Dedekind domains.

Theorem 6.48. *For an integral domain R , the following conditions are equivalent:*

- (1) *Every non-zero ideal of R is invertible.*
- (2) *R is either a field or a Noetherian, normal ring of dimension 1.*
- (3) *R is Noetherian, and for each maximal ideal $\mathfrak{m} \subset R$, $R_{\mathfrak{m}}$ is a DVR.*

Proof. Proof of (1) implies (2): Consider $R_{\mathfrak{m}}$ for a maximal ideal $\mathfrak{m} \subset R$. Every ideal in $R_{\mathfrak{m}}$ is invertible, hence is principal. So $R_{\mathfrak{m}}$ is local principal ideal domain, so if it is not a field, then it is a DVR, hence Noetherian, normal ring of dimension 1 by Theorem 6.38.

Proof of (2) implies (3): If R is Noetherian and normal ring of dimension 1, then $R_{\mathfrak{m}}$ is a Noetherian, local, normal of dimension 1, hence by Theorem 6.38, $R_{\mathfrak{m}}$ is a DVR.

Proof of (3) implies (1): Given $I \subset R$ suppose, for contradiction, $II^{-1} \neq R$, then let $II^{-1} \subset \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Since $R_{\mathfrak{m}}$ is a PID, we can find an element $t \in I$ such that $\frac{t}{1}$ is a generator of the invertible ideal $S^{-1}I = I_{\mathfrak{m}}$ for $S = R \setminus \mathfrak{m}$. We let $I = (a_1, \dots, a_r)$ as R is Noetherian. There exist elements $s_i \in R \setminus \mathfrak{m}$ such that $s_i a_i \in (t) \subset R$. Let $s = s_1 s_2 \dots s_r$, then $st^{-1} \in I^{-1}$. But now, $s = st^{-1}t \in I^{-1}I \subset \mathfrak{m}$, a contradiction. \square

◁ Consider the subring $R = \mathbb{Z} + 2i\mathbb{Z}$ of Gaussian integers. Show that the ideal $I = 2\mathbb{Z}[i]$ is non-invertible in R (but it is invertible in $\mathbb{Z}[i]$).

End of lec. 26

Theorem 6.49. *In a Dedekind domain, every non-zero ideal of R can be written (uniquely) as a product of a finite number of prime ideals.*

Proof. If there are non-zero ideals which are not products of prime ideals, we can assume that I is maximal among them. Let $\mathfrak{p} \supset I$ be a prime ideal containing it, then $I\mathfrak{p}^{-1} \subset R$ is an ideal, strictly containing I ; for $I\mathfrak{p}^{-1} = I$ would imply $\mathfrak{p}^{-1} = R$ on multiplying by I^{-1} . Hence $I\mathfrak{p}^{-1}$ is a product of prime ideals, and since $I = (I\mathfrak{p}^{-1})\mathfrak{p}$, we get a contradiction.

If $I = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m = \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_n$ with all \mathfrak{p}_i and \mathfrak{q}_j prime, then $\mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_n \subset \mathfrak{p}_1$, so some $\mathfrak{q}_i \subset \mathfrak{p}_1$. Since all non-zero prime ideals are maximal, we must have $\mathfrak{q}_i = \mathfrak{p}_1$, so we can cancel these from both sides and continue until we obtain the uniqueness result. \square

Conversely, that is, if R is a domain that has the property that every ideal is a product of prime ideals, then one can prove that R is a Dedekind ring. This is a theorem of Matusita, which we do not have time to prove.⁷

Corollary 6.50. *If R is a Dedekind domain, the non-zero fractional ideals of R form an abelian group with respect to multiplication. It is freely generated by the non-zero prime ideals of R .*

⁷A proof can be found in Theorem 11.6 of Matsumura's book.

The **ideal class group** of R is the quotient of this free abelian group by the group of principal fractional ideals. This turns out to be a very important finite abelian group that you would study if you took an Algebraic Number Theory course.

6.6 Completion

Recall from your analysis course that \mathbb{R} is constructed as a completion of \mathbb{Q} using the distance function $d(x, y) = |x - y|$. This construction goes via Cauchy sequences. We can adapt this in ring theory. We begin with the setting of discrete valuation rings.

Let K be a field and $\nu : K \rightarrow \mathbb{Z} \cup \{\infty\}$ be a discrete valuation. Let $r \in \mathbb{R}$ with $r > 1$. We set

$$|x|_\nu = r^{-\nu(x)}, \text{ for } x \in K.$$

We can verify that $|\cdot| : K \rightarrow \mathbb{R}_{\geq 0}$ is a **norm** on K . Namely, the following properties are satisfied:

$$\begin{aligned} |xy|_\nu &= |x|_\nu |y|_\nu \\ |x + y|_\nu &\leq \max\{|x|_\nu, |y|_\nu\} \\ |x|_\nu = 0 &\iff x = 0 \end{aligned}$$

The second property is called the non-archimedean property. Note that, in particular, it implies the triangular inequality $|x + y|_\nu \leq |x|_\nu + |y|_\nu$. Hence, we can define a distance function $d(x, y) = |x - y|_\nu$ and in turn equip K with a topology with basic open sets $B_{x_0, \epsilon} = \{x \in K : |x - x_0|_\nu < \epsilon\}$. We next show that in non-archimedean geometry every triangle is isosceles!

Lemma 6.51. *If $|x|_\nu < |y|_\nu$ then $|x - y|_\nu = |y|_\nu$.*

Proof. We have $|x - y|_\nu \leq \max\{|x|_\nu, |y|_\nu\} = |y|_\nu$ since $|x|_\nu < |y|_\nu$. On the other hand, $y = (y - x) + x$, hence $|y|_\nu \leq \max\{|x - y|_\nu, |x|_\nu\} = |x - y|_\nu$ since $|x|_\nu < |y|_\nu$. \square

Recall that a sequence $(x_n)_{n \geq 1}$ is a **Cauchy sequence** if $\forall \epsilon > 0, \exists n_0 \geq 1$ such that $|x_n - x_m|_\nu < \epsilon$ for all $n, m \geq n_0$. In terms of the valuation, this is equivalent to the condition that for all $N > 0, \exists n_0 \geq 1$ such that $\nu(x_n - x_m) > N$ for all $n, m \geq n_0$.

We say that a sequence $(x_n)_{n \geq 1}$ converges to a **limit** x if $\forall \epsilon > 0, \exists n_0 \geq 0$ such that $|x_n - x|_\nu < \epsilon$ for all $n \geq n_0$. Or equivalently, $\forall N > 0, \exists n_0 \geq 0$ such that $\nu(x_n - x) > N$ for all $n \geq n_0$.

A field K is called **complete** with respect to valuation if every Cauchy sequence has a limit.

Let K_ν be a field with a valuation. We say that a field $\hat{K}_\nu \supset K_\nu$ such that the valuation ν extends to \hat{K}_ν is a **completion** of K_ν if \hat{K}_ν is complete and is the closure of K_ν with respect to the topology induced by ν .

Given a field K_ν with a valuation ν , there is a canonical construction of a completion of the K_ν . We next outline the construction.

We let

$$\mathcal{C}_\nu := \{(x_n)_{n \geq 1} : x_n \in K, (x_n) \text{ a Cauchy sequence}\},$$

and

$$\mathcal{I}_\nu := \{(x_n)_{n \geq 1} \in \mathcal{C}_\nu : \lim_{n \rightarrow \infty} x_n = 0\}.$$

► \mathcal{C}_ν is a commutative ring with $(x_n) \pm (y_n) = (x_n \pm y_n)$, $(x_n) \cdot (y_n) = (x_n y_n)$, $0 = (0)_{n \geq 1}$ and $1 = (1)_{n \geq 1}$.

► \mathcal{I}_ν is a maximal ideal in \mathcal{C}_ν , hence $\hat{K}_\nu := \mathcal{C}_\nu / \mathcal{I}_\nu$ is a field. We have that the map $K_\nu \rightarrow \hat{K}_\nu$ given by $x \rightarrow (x)_{n \geq 1}$ is an embedding, hence $K_\nu \subset \hat{K}_\nu$ is a field extension.

Lemma 6.52. *Let $0 \neq \alpha \in \hat{K}_\nu$ represented by $(x_n)_{n \geq 1} \in \mathcal{C}_\nu / \mathcal{I}_\nu$. Then there exists an $n_0 \geq 1$ such that $\nu(x_n) = \nu(x_{n_0})$ for all $n \geq n_0$. We define $\hat{\nu} : \hat{K}_\nu \rightarrow \mathbb{Z} \cup \{\infty\}$ by letting $\hat{\nu}(\alpha) = \lim_{n \rightarrow \infty} \nu(x_n) = \nu(x_{n_0})$. Then, $\hat{\nu}$ is a valuation extending ν .*

Proof. Since $\alpha \neq 0$, $(x_n) \notin \mathcal{I}_\nu$. Hence, there exists $c > 0$ such that for all $n \geq 1$, there exists $i_n > n$ with $\nu(x_{i_n}) \leq c$. On the other hand, (x_n) is a Cauchy sequence, therefore, there exists $N \geq 1$ such that $\nu(x_n - x_m) > c$ for all $n, m \geq N$. Let $n_0 = i_N > N$. Then, for all $n \geq n_0$, we have

$$\nu(x_n) = \nu(x_n - x_{n_0} + x_{n_0}) \geq \min\{\nu(x_n - x_{n_0}), \nu(x_{n_0})\} = \nu(x_{n_0})$$

and

$$\nu(x_{n_0}) = \nu(x_{n_0} - x_n + x_n) \geq \min\{\nu(x_{n_0} - x_n), \nu(x_n)\} = \nu(x_n)$$

Hence, $\nu(x_n) = \nu(x_{n_0})$ for all $n \geq n_0$. We define $\hat{\nu}(\alpha) := \nu(x_{n_0})$. We leave it as an exercise to check that $\hat{\nu}$ is well-defined and a valuation. \square

$\hat{\nu} : \hat{K}_\nu \rightarrow \mathbb{Z} \cup \{\infty\}$ is a valuation such that all the Cauchy sequences in \hat{K}_ν converge. In particular, if $\alpha \in \hat{K}_\nu$ is represented by $(x_n)_{n \geq 1} \in \mathcal{C}_\nu / \mathcal{I}_\nu$ then $\lim_{n \rightarrow \infty} x_n = \alpha$.

Let $\hat{R}_\nu = \{x \in \hat{K}_\nu : \hat{\nu}(x) \geq 0\}$ be the corresponding discrete valuation ring in \hat{K}_ν . Let $t \in R_\nu$ such that $\nu(t) = 1$. We have seen that $\mathfrak{m}_\nu = (t)$ is the maximal ideal of R_ν . Since $\hat{\nu}|_{R_\nu} = \nu$, we have $\hat{\nu}(t) = 1$ and $\hat{\mathfrak{m}}_\nu = (t)$ is the unique maximal ideal of \hat{R}_ν . Thus, we have a diagram

$$\begin{array}{ccccc} K_\nu & \supset & R_\nu & \supset & \mathfrak{m}_\nu \\ & & \cap & & \cap \\ \hat{K}_\nu & \supset & \hat{R}_\nu & \supset & \hat{\mathfrak{m}}_\nu \end{array}$$

◁ Show that the completion of the discrete valuation ring $k[X]_{(X)}$ is isomorphic to $k[[X]]$ the formal power series ring.

We define an infinite sum $\sum_{n \geq 0} x_n$ if the partial sums $s_N = \sum_{n \geq 0}^N x_n$ converges. In a complete discrete valuation ring \hat{R}_ν , the sum converges if and only if $\lim_{n \rightarrow \infty} x_n = 0$. Indeed, if $x_n \rightarrow 0$, the partial sums form a Cauchy sequence since

$$|s_N - s_M| = |x_{N+1} + \dots + x_M| \leq \max_{N < n \leq M} |x_n|$$

and conversely if s_N converge, $s_N - s_{N-1} = x_N \rightarrow 0$.

Proposition 6.53. *Let $A \subset R_\nu$ be a set of representatives of $k_\nu = R_\nu/\mathfrak{m}_\nu$, then every element of \hat{R}_ν can be written uniquely as $\sum_{m=0}^{\infty} a_m t^m$ with $a_n \in A$ where a representative Cauchy sequence $(x_n)_{\geq 0}$ is given by the partial sums $x_n = \sum_{m=0}^n a_m t^m$.*

Proof. Let $x \in \hat{R}_\nu$ given. There is exactly one $a_0 \in A$ such that $|x - a_0|_\nu < 1$. Then, we let $x = a_0 + tb_1$ for some $b_1 \in \hat{R}_\nu$. Then, there is exactly one $a_1 \in A$ such that $|b_1 - a_1|_\nu < 1$, and then $b_1 = a_1 + tb_2$ for some $b_2 \in \hat{R}_\nu$. In this way, we get for every n , $x = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n + b_{n+1} t^{n+1}$ with $a_i \in A$ and $b_{n+1} \in \hat{R}_\nu$. Now, $b_{n+1} t^{n+1} \rightarrow 0$, hence $x = \sum_{m=0}^{\infty} a_m t^m$. \square

Thus, given two elements $x = \sum_{m=0}^{\infty} a_m t^m, y = \sum_{m=0}^{\infty} b_m t^m$, using the addition and multiplication in R_ν , we can write

$$\begin{aligned} \sum_{m=0}^{\infty} a_m t^m + \sum_{m=0}^{\infty} b_m t^m &= \sum_{m=0}^{\infty} c_m t^m, \\ \left(\sum_{m=0}^{\infty} a_m t^m \right) \left(\sum_{m=0}^{\infty} b_m t^m \right) &= \sum_{m=0}^{\infty} d_m t^m \end{aligned}$$

However, in general, determining $(c_m)_{m \geq 0}$ and $(d_m)_{m \geq 0}$ from $(a_m)_{m \geq 0}$ and $(b_m)_{m \geq 0}$ can be quite complicated. In particular, the above proposition does not mean that every \hat{R}_ν is isomorphic to $k_\nu[[t]]$.

On the other hand, if we want to compute c_m and d_m for all $m \leq n$ for some fixed n , we can do this in R_ν by working modulo t^n , thanks to the following isomorphism of rings.

\triangleleft For all $n \geq 1$, $R_\nu/t^n R_\nu \simeq \hat{R}_\nu/t^n \hat{R}_\nu$.

Let p be prime number consider the discrete valuation ring $\mathbb{Z}_{(p)}$ with the valuation $\nu_p : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$ given by $\nu(\frac{a}{b}) = n$ if $\frac{a}{b} = p^n \frac{a'}{b'}$ with $p \nmid a'$ and $p \nmid b'$. By definition, the **field of p -adic numbers** is $\mathbb{Q}_p = \hat{\mathbb{Q}}_{\nu_p}$ and we define **p -adic integers** as

$$\mathbb{Z}_p := \{a \in \mathbb{Q}_p : \hat{\nu}_p(a) \geq 0\}$$

which is a local ring with maximal ideal (p) , and $\mathbb{Z}_p/(p) \simeq \mathbb{F}_p$.

\triangleleft Show that $\mathbb{Z}[[X]]/(X - p)$ is isomorphic to \mathbb{Z}_p .

Let us now consider the equation $X^5 = X$ in \mathbb{Z}_5 . In $\mathbb{F}_5 = \mathbb{Z}_5/(5)$ the solutions are $\{0, 1, 2, 3, 4\}$. We wish to “lift” these solutions to \mathbb{Z}_5 . Clearly, 0 and 1 in \mathbb{Z}_5 lifts the solutions 0 and 1 in \mathbb{F}_5 and

$$-1 = 4 + 4 \cdot 5 + 4 \cdot 5^2 + \dots \in \mathbb{Z}_5$$

lifts $4 \in \mathbb{F}_5$. Let's lift, for example, $2 \in \mathbb{F}_5$. We are looking to solve the equation

$$(2 + a_1 5 + a_2 5^2 + \dots)^4 = 1 \in \mathbb{Z}_5 \quad \text{with} \quad a_i \in \{0, 1, 2, 3, 4\}$$

We can try this level by level by looking at the equation in $\mathbb{Z}_5/\mathfrak{m}^s \simeq \mathbb{Z}/5^s$ for $s = 1, 2, \dots$. For example, $(2 + a_1 5)^4 = 1 \in \mathbb{Z}/25$ gives the equation $16 + 10a_1 = 1 \in \mathbb{Z}/25$. Thus, we have $a_1 = 1$. Next, we look at $(2 + 1 \cdot 5 + a_2 5^2)^4 = 1 \in \mathbb{Z}/125$, and this simplifies to $26 + 50a_2 = 1 \in \mathbb{Z}/125$. Thus, we have $a_2 = 2$. Next, we look at the equation $(2 + 1 \cdot 5 + 2 \cdot 5^2 + a_3 5^3)^4 = 1 \in \mathbb{Z}/625$ which reduces to $376 + 250a_3 = 1 \in \mathbb{Z}/625$, hence $a_3 = 1$. Thus, we arrived at

$$(2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \dots)^4 = 1 \in \mathbb{Z}_5$$

as the root lifting 2. Similarly, one can compute

$$(3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \dots)^4 = 1 \in \mathbb{Z}_5$$

as the root lifting 3. Though, we can also notice that these two numbers are additive inverses.

We next prove a version of Hensel's lemma which is a generic term for results which infer the existence of a solution in \hat{K}_ν from an approximate solution using Newton's method.

Lemma 6.54. (*Hensel's lemma*) *Let $f \in R_\nu[X]$, $f = \sum_{i=0}^n a_i X^i$ and $a_n \notin \mathfrak{m}_\nu$. Let $\bar{\cdot} : R_\nu \rightarrow R_\nu/\mathfrak{m}_\nu = k_\nu$ is reduction homomorphism to the residue field, and $\bar{f} = \sum_{i=0}^n \bar{a}_i X^i \in k_\nu[X]$. Suppose that there exists $\bar{x}_0 \in k_\nu$ such that*

$$\bar{f}(\bar{x}_0) = 0 \quad \text{and} \quad \bar{f}'(\bar{x}_0) \neq 0, \tag{3}$$

where $f'(X) = \sum_{i=1}^n i a_i X^{i-1}$ is the (formal) derivative. Then, there exists a unique root x of f in \hat{K}_ν , satisfying $|x - x_0| < |f'(x_0)|$.

Furthermore, $|x - x_0| = |f(x_0)|/|f'(x_0)| < |f'(x_0)|$ and $|f'(x)| = |f'(x_0)|$.

Proof. Let $x_0 \in R_\nu$ be any lift of $\bar{x}_0 \in k_\nu$. We have $f(x_0) \in \mathfrak{m}_\nu$ but $f'(x_0) \notin \mathfrak{m}_\nu$ so $|f(x_0)| < 1$ and $|f'(x_0)| = 1$. In particular, we have

$$|f(x_0)| < |f'(x_0)|^2 \tag{4}$$

and in fact this is the only condition we will use in the rest of the proof, so the assumption (3) can be replaced with the weaker assumption (4).

Since $|\frac{f(x_0)}{f'(x_0)}| < |f'(x_0)| \leq 1$, there exists $y_0 \in \mathfrak{m}_\nu$ such that $f(x_0) + y_0 f'(x_0) = 0$.

Let us define polynomials $f_1, f_2, \dots \in R_\nu[X]$ via the identity

$$f(X + Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \dots$$

Then $f_1(X) = f'(X)$.

We have

$$|f(x_0 + y_0)| \leq \max_{j \geq 2} |f_j(x_0) y_0^j|$$

Here, $|f_j(x_0)| \leq 1$ since $f_j[X] \in R_\nu[X]$ and $y_0 \in R_\nu$. Hence,

$$|f(x_0 + y_0)| \leq |y_0|^2 = \frac{|f(x_0)|^2}{|f'(x_0)|^2} < |f(x_0)|$$

Similarly,

$$|f'(x_0 + y_0) - f'(x_0)| \leq |y_0| < |f'(x_0)|$$

and so $|f'(x_0 + y_0)| = |f'(x_0)|$ by the non-archimedean property of the norm.

We now put $x_1 = x_0 + y_0$ and note that $|f(x_1)| < |f'(x_1)|^2$, so we can repeat this process.

In this way, we obtain a sequence $(x_n)_{n \geq 0}$ using Newton's formula $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ with the properties

(i) $|x_n| \leq 1$ hence $x_n \in R_\nu$.

(ii) $|f'(x_n)| = |f'(x_0)|$

(iii) $|f(x_{n+1})| \leq \frac{|f(x_n)|^2}{|f'(x_n)|^2} = \frac{|f(x_n)|^2}{|f'(x_0)|^2} < |f(x_n)|$ and so $f(x_n) \rightarrow 0$ as $n \rightarrow \infty$.

(iv) $|x_{n+1} - x_n| = |y_n| = \frac{|f(x_n)|}{|f'(x_n)|} = \frac{|f(x_n)|}{|f'(x_0)|} \rightarrow 0$ as $n \rightarrow \infty$.

It follows that $(x_n)_{n \geq 0}$ is a Cauchy sequence with respect to ν . Then, the element $x := \lim_{n \rightarrow \infty} x_n \in \hat{K}_\nu$ exists and $f(x) = 0$.

To see that $|x - x_0| = |f(x_0)|/|f'(x_0)|$, let us observe that

$$|x_{n+1} - x_n| = \frac{|f(x_n)|}{|f'(x_n)|} < \frac{|f(x_0)|}{|f'(x_0)|}$$

for all $n \geq 1$. Now, note that $|x_1 - x_0| = |f(x_0)|/|f'(x_0)|$ and if $|x_n - x_0| = |f(x_0)|/|f'(x_0)|$ for some n , then it follows that $|x_{n+1} - x_0| = |f(x_0)|/|f'(x_0)|$ since we have $|x_{n+1} - x_0| = |x_n - x_0|$ by Lemma 6.51.

Finally to see the uniqueness, suppose \tilde{x} is another solution with $|\tilde{x} - x_0| < |f'(x_0)|$ and $x \neq \tilde{x}$. Then, let $\tilde{y} = x + \tilde{y}$. We have

$$0 = f(x + \tilde{y}) - f(x) = f'(x)\tilde{y} + f_2(x)\tilde{y}^2 + \dots$$

But, $|\tilde{y}| = |x - x_0 + x_0 - \tilde{x}| \leq \max\{|x - x_0|, |\tilde{x} - x_0|\} < |f'(x_0)| = |f'(x)|$ and $|f_i(x)| \leq 1$, the first term on the right side of the above equation has strictly greater norm than the others, hence the sum cannot be 0, which is a contradiction. \square

► The method used in Hensel's lemma is the adaptation of Newton's method of approximations to the roots of a real polynomial, where successive approximations are defined by the formula $x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})}$. However, in the non-archimedean setting it's guaranteed that the sequence converges, whereas in the real case, it usually converges but not always. For example, if you take $f(x) = x^3 - x$ and choose $x_0 = \frac{1}{\sqrt{5}}$, then we get $x_i = \frac{(-1)^i}{\sqrt{5}}$ for all $i \geq 0$.

Corollary 6.55. Consider $f(X) = X^{p-1} - 1 \in \mathbb{Z}[X] \subset \mathbb{Z}_p[X]$. Then, for every $\xi \in \mathbb{F}_p^\times$ there exists a unique $[\xi] \in \mathbb{Z}_p$ such that $f([\xi]) = 0$ and $[\xi] = \xi \in \mathbb{Z}_p/(p) = \mathbb{F}_p$.

Proof. We have $f'(\xi) = (p-1)\xi^{p-2} \neq 0 \in \mathbb{F}_p$. $\bar{f}(X) = X^{p-1} - 1 = \prod_{0 \neq x \in \mathbb{F}_p} (X - x)$. Hence, by Hensel, f has a root in \mathbb{Z}_p lifting ξ . \square

We have seen above that in \mathbb{Z}_5 , we have $[1] = 1 + 0 \cdot 5 + 0 \cdot 5^2 + 0 \cdot 5^3 + \dots$, $[2] = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \dots$, $[3] = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \dots$, $[4] = 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \dots$.

Putting $[0] = 0$, it follows that $A = \{[0], [1], [2], \dots, [p-1]\} \subset \mathbb{Z}_p$ give a complete set of representatives of $\mathbb{F}_p = \mathbb{Z}_p/(p)$, hence any element of \mathbb{Z}_p can be written uniquely as

$$\sum_{m=0}^{\infty} [a_m] p^m,$$

where $[a_m] \in A$. This is called the Teichmüller representation. This representation is preferable over $\{0, 1, 2, \dots, p-1\}$ due the following result.

Theorem 6.56. (Witt) There exist polynomials $P_n, Q_n \in \mathbb{Z}[X_0, X_1, \dots, X_n, Y_0, Y_1, \dots, Y_n]$ such that given $a_0, \dots, a_n, b_0, \dots, b_n \in \mathbb{F}_p$ if we define $c_n = P_n(a_0, \dots, a_n, b_0, \dots, b_n)$ and $d_n = Q_n(a_0, \dots, a_n, b_0, \dots, b_n)$, then

$$\sum_{m=0}^{\infty} [a_m] t^m + \sum_{m=0}^{\infty} [b_m] t^m = \sum_{m=0}^{\infty} [c_m] t^m,$$

$$\left(\sum_{m=0}^{\infty} [a_m] t^m \right) \cdot \left(\sum_{m=0}^{\infty} [b_m] t^m \right) = \sum_{m=0}^{\infty} [d_m] t^m$$

We won't prove this theorem⁸ but we list the first few polynomials:

$$P_0(X_0, Y_0) = X_0 + Y_0,$$

$$P_1(X_0, X_1, Y_0, Y_1) = X_1 + Y_1 - (X_0^{p-1} Y_0 + X_0^{p-2} Y_0^2 + \dots + X_0 Y_0^{p-1}),$$

$$Q_0(X_0 Y_0) = X_0 Y_0,$$

$$Q_1(X_0, X_1, Y_0, Y_1) = X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1.$$

► Our discussion of Witt vectors was a bit simplified since in our example of \mathbb{Z}_p the residue field is $k = \mathbb{F}_p$. If the residue field is a more general perfect field of characteristic p , then one represents the elements of the ring as $\sum_{m=0}^{\infty} [a_m] p^{-m} t^m$ and the addition and multiplication formulae above continue to hold.

End of lec. 28

A more general construction of a completion of a ring can be defined as follows Let $I \subset R$ be an ideal. As mentioned before, we can use this to define I -adic topology on R .

⁸You can find a proof in Serre - Local fields

Definition 6.57. Given an ideal $I \subset R$, we define I -adic topology on R by declaring I^i for $i \geq 1$ to be a system of open neighborhoods of 0 and asking R to be a topological group under addition (so that the cosets $x + I^i$ for $i \geq 1$ and $x \in R$ form a basis of this topology). More generally, given an R -module M , we can consider the chain of submodules

$$M = M \supset IM \supset I^2M \supset \dots$$

For any $x \in M$, we take $\{x + I^iM\}$ as a basis of topology on M called the I -adic topology. The addition $M \times M \rightarrow M$ and the multiplication $R \times M \rightarrow M$ are continuous (where R is assumed to be equipped with the I -adic topology.)

► A sequence $a_n \in M$ converges to a if and only if for any i there exists $N \geq 1$ such that $a_n - a \in I^iM$ for all $n \geq N$.

► The complement of the coset $x + I^iM$ is open, hence $x + I^iM$ is both open and closed.

In general, the topology defined on M does not have to be Hausdorff.

< Show that the closure of a subset S of M is equal to $\bigcap_{i=1}^{\infty} (S + I^iM)$. In particular, the closure of $\{0\}$ in the I -adic topology is $\bigcap_{i=1}^{\infty} I^iM$. Deduce that the topology on M is Hausdorff if and only if $\bigcap_{i=1}^{\infty} I^iM = \{0\}$. (In particular, if R is a local Noetherian ring and M is Noetherian, then every I -adic topology on M is Hausdorff by Krull's intersection theorem.)

On an R -module M equipped with an I -adic topology, fixing $r \in \mathbb{R}$ with $r > 1$, we can define a distance function $d(x, y) = r^{-n}$ if $x - y \in I^nM$ but $x - y \notin I^{n+1}M$. This gives a metric space if and only if the topology on M is Hausdorff.

We can now define the completion of R in I -adic topology using Cauchy sequences (as we did in the case of DVRs). However, it turns out that there is a more convenient algebraic construction of this completion which we will discuss first. Let us consider the product ring

$$\prod_{i \geq 1} R/I^i = \{(x_i) : x_i \in R/I^i\}$$

Recall that a basis of open sets in the product topology is given by

$$\prod_{i \in F} U_i \times \prod_{i \in F^c} R/I^i$$

where $F \subset \mathbb{Z}_{>0}$ is a finite set and F^c is the complement of F in $\mathbb{Z}_{>0}$. Equivalently, product topology is determined by the condition that $\pi_i : \prod_{i \geq 1} R/I^i \rightarrow R/I^i$ is continuous for all i .

For $j > i$, we have a quotient maps $R/I^j \rightarrow R/I^i$, and we can form an inverse limit using these maps as follows

Definition 6.58. Define $\widehat{R}_I = \varprojlim_i R/I^i$, the I -adic completion to be

$$\widehat{R} = \{(x_i) \in \prod_{i \geq 1} R/I^i : x_j - x_i \in I^i \text{ for all } j > i\}$$

equipped with the subspace topology.

There is a continuous ring homomorphism $R \rightarrow \widehat{R}_I$ given by $r \rightarrow (r, r, r, \dots)$. Using this, we can extend ideals $J \subset R$ to ideals $\widehat{R}_I J$ in \widehat{R}_I .

The images of I^i are given by ideals $\widehat{I}^i = \{(x_i) \in \widehat{R}_I : x_j = 0 \text{ for all } j \leq i\}$. It follows that $\widehat{R}_I/\widehat{I}^i = R/I^i$. Note that $\bigcap_{i=1}^{\infty} \widehat{I}^i = (0)$ in \widehat{R}_I .

< Show that the map $R \rightarrow \widehat{R}_I$ is injective if $\bigcap_{i=1}^{\infty} I^i = (0)$.

We say that R is **I -adically complete** if $R \rightarrow \widehat{R}_I$ is an isomorphism. In this case, if $I = \mathfrak{m}$ is a maximal ideal, we say that R is a **complete local ring**. This is justified because of the following proposition.

Proposition 6.59. *If R is I -adically complete, then I lies in the Jacobson radical $\mathcal{J}(R)$.*

Proof. Pick any $a \in I$. The partial sums of the geometric series $\sum_{n \geq 0} a^n$ form a Cauchy sequence. Hence, it has a limit b . Then $(1 - a)b = (1 - a)\sum_{n \geq 0} a^n = 1$ so $(1 - a)$ is a unit. Therefore, $a \in \mathcal{J}(R)$. \square

In particular, this implies that if R is \mathfrak{m} -adically complete for a maximal ideal \mathfrak{m} , then R is local.

Let's consider an example. Let $R = k[x]$ and $I = (x)$, then

$$R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow$$

is as follows

$$k \leftarrow k[x]/(x^2) \leftarrow k[x]/(x^3) \leftarrow \dots$$

A typical element looks like as follows:

$$a_0 \leftarrow a_0 + a_1x \leftarrow a_0 + a_1x + a_2x^2 \leftarrow \dots$$

We see that \widehat{R}_I can be identified as a ring with the power series ring $k[[x]]$.

Similarly, one can prove that the \mathfrak{m} -adic completion of $k[X_1, \dots, X_n]$ at the maximal ideal $\mathfrak{m} = (X_1, \dots, X_n)$ is $k[[X_1, \dots, X_n]]$.

Corollary 6.60. *An element $f \in k[[X_1, X_2, \dots, X_n]]$ is a unit if and only if the constant term of f is non-zero.*

Proof. $k[[X_1, \dots, X_n]]$ is a complete local ring with maximal ideal (X_1, \dots, X_n) . The complement of the maximal ideal is precisely the elements with non-zero constant term. \square

For k a field, consider the ring map $k[X] \rightarrow k[X, Y]/(Y^2 - X - 1)$ sending $X \rightarrow X$. Upon considering the spectrums, this gives us a 2-to-1 map of affine varieties $\pi : V \rightarrow \text{Spec } k$, where $V = \mathcal{V}(Y^2 - X - 1)$. If we concentrate near the points $(0, -1)$ and $(0, 1)$ in V corresponding to the maximal ideals $(X, Y + 1)$ and $(X, Y - 1)$ in $k[X, Y]$ we see that these map to $0 \in \text{Spec } k$ corresponding to the maximal ideal $(X) \subset k[X]$. Thus, there is no inverse to π , we know from analysis that the inverse can only exist locally near $(0, 1)$ or $(0, -1)$ and would be given by

$X \rightarrow (X, \pm\sqrt{X+1})$. We can make sense of such maps if we complete our rings. To focus near $(0, -1)$, we first change co-ordinates $(X, Y) \rightarrow (X, Y - 1)$, and consider the map $k[X] \rightarrow k[X, Y]/(Y^2 - 2Y - X)$ given by $X \rightarrow X$ so that in the new co-ordinates $(0, 0) \in V$ maps to $0 \in \text{Spec} k$ and we complete near these points to get a map of rings $k[[X, Y]]/(Y^2 - 2Y - X) \rightarrow k[[X]]$, given by $X \rightarrow X, Y \rightarrow -\frac{X}{2} + \frac{X^2}{8} + \dots$ where the latter is the power series expansion of $1 - \sqrt{X+1}$ around $X = 0$ (which even converges for $|x| < 1$ over $k = \mathbb{C}$).⁹

► Let us note that the completion of a ring R with respect to an ideal I can also be constructed using Cauchy sequences as we did in the case of completions of DVRs. Consider the Cauchy sequences for the I -adic topology, $\mathcal{C}_I(R)$, by definition these are sequences $(x_n)_{n \geq 1}$ such that for all $N > 0$, there exists $n_0 \geq 1$ such that for all $n, m \geq n_0$, $x_n - x_m \in I^N$. We also write $\mathcal{I}_I(R)$ the be the ideal in $\mathcal{C}_I(R)$ of Cauchy sequences that converge to 0. Given a Cauchy sequence $(x_n)_{n \geq 1}$ we can look the $x_n + I^i$ in R/I^i . For large n , the sequence $x_n + I$ stabilise by the property of being a Cauchy sequence, and so we can construct a map $\mathcal{C}_I(R) \rightarrow R/I^i$ by sending a Cauchy sequence to the stable value. One can show that this gives rise to a ring homomorphism $\mathcal{C}_I(R) \rightarrow \widehat{R}$ with kernel $\mathcal{I}_I(R)$.

◁ Let R_ν be a discrete valuation ring determined by $\nu : K_\nu \rightarrow \mathbb{Z} \cup \{\infty\}$ and maximal ideal \mathfrak{m}_ν . Show that the topology on K_ν determined by the norm function $|x|_\nu = r^{-\nu(x)}$ for $r \in \mathbb{R}$ with $r > 1$ on R restricts to the \mathfrak{m}_ν -adic topology on R_ν .

Definition 6.61. For an R -module M , we define I -adic completion of M as $\widehat{M}_I = \varprojlim_i M/I^i M$.

More explicitly,

$$\widehat{M}_I = \{(x_i) \in \prod_{i \geq 1} M/I^i M : x_j - x_i \in I^i M \text{ for all } j > i\}$$

equipped with the subspace topology.

If M is a Noetherian module, and N is a submodule, then one can understand the statement of Artin-Rees lemma as saying that the I -adic topology on N coincides with the topology of N as a subspace of M when M itself is equipped with I -adic topology.

◁ Let $A = \mathbb{Z}$, $M = \mathbb{Z}$, $N = 4\mathbb{Z}$ and $I = (2)$. Compute the filtrations $N \supset IN \supset I^2 N \supset \dots$ and $N \supset N \cap IM \supset N \cap I^2 M \supset \dots$. Show directly that the induced topologies on N are the same.

Theorem 6.62. Let R be Noetherian and I and J be ideals of R , then $\widehat{J}_I = \widehat{R}_I J$ and $\widehat{R}_I / \widehat{J}_I = \widehat{(R/J)}_I$

◁ We leave the proof of this theorem as an exercise. Observe that the kernel of the R -module homomorphism $I^n \rightarrow (I^n + J)/J$ is $I^n \cap J$ and combine this with Artin-Rees lemma to deduce

⁹In the book [Eisenbud - Commutative Algebra], this example is discussed in the beginning of Chapter 7, where the completion of $k[X, Y]/(Y^2 - X - 1)$ at the ideal $(X, Y + 1)$ is described as $k[[X, Y]]/(Y^2 - X - 1)$. This is not quite correct: $Y^2 - X - 1$ is invertible in $k[[X, Y]]$, hence $k[[X, Y]]/(Y^2 - X - 1)$ is trivial. Moreover, one cannot define a ring map $k[[X, Y]]/(Y^2 - X - 1) \rightarrow k[[X]]$ via $X \rightarrow X, Y \rightarrow -1 - \frac{X}{2} + \frac{X^2}{8} + \dots$ as written there, since if such a map existed where would $1 + Y + Y^2 + \dots$ go under this map? The constant term of the image of this map is a sum like $1 - 1 + 1 - 1 + 1 \dots$

that I -adic completion of J can also be computed using the completion given with respect to submodules of J defined by $I^n + J$ for $n \geq 0$. (see Theorem 8.11 in Matsumura - Commutative Ring Theory if you get stuck).

Corollary 6.63. *The completion of $k[X_1, \dots, X_n]/J$ at the maximal ideal $I = (X_1, \dots, X_n)$ is given by $k[[X_1, \dots, X_n]]/J$.*

More generally, we have the following result

Theorem 6.64. *Let R be a Noetherian ring and $I = (f_1, \dots, f_n)$ be an ideal. Then I -adic completion of R is isomorphic to $R[[T_1, \dots, T_n]]/(T_1 - f_1, \dots, T_n - f_n)$.*

Proof. Let $A = R[T_1, \dots, T_n]$ and $J = (T_1 - f_1, \dots, T_n - f_n) \subset A$. Then $A/J = R$. Let $I' = (T_1, \dots, T_n) \subset A$. Then I' -adic topology on R considered as an A -module coincides with the I -adic topology on A . Hence

$$\widehat{R}_I = \widehat{R}_{I'} = \widehat{A}_{I'}/\widehat{J}_{I'} = \widehat{A}_{I'}/J\widehat{A}_{I'} = R[[T_1, \dots, T_n]]/(T_1 - f_1, \dots, T_n - f_n)$$

□

◁ Let $R = k[X, Y]/(Y^2 - X^3 - X^2)$ and $I = (X, Y)$. Show that R is an integral domain but the I -adic completion \widehat{R} is not an integral domain.

◁ Prove the following version of Hensel's lemma: Suppose R is local with maximal ideal \mathfrak{m} and that R is \mathfrak{m} -adically complete. Let $f \in R[X]$ be monic polynomial and its reduction $\bar{f} \in R/\mathfrak{m}[X]$ can be factorised as $\bar{f} = \bar{g}\bar{h}$ for some polynomials $\bar{g}, \bar{h} \in R/\mathfrak{m}[X]$ then there exist lifts $g, h \in R[X]$ such that $f = gh \in R[X]$.

We finish by stating a characterisation of complete local Noetherian rings:

Theorem 6.65. *(Cohen Structure Theorem) Let R be a complete local Noetherian ring with maximal ideal \mathfrak{m} and residue field $k = R/\mathfrak{m}$. If R contains a field (as a subring), then $R \cong k[[X_1, \dots, X_n]]/I$ for some n and ideal I .*

The proof is beyond our scope here but you can find the proof of this theorem and its generalisations in Section 29 of Matsumura's book.

End of lec. 29

7 A quick list of things that we left out

Primary decomposition. We proved that every radical ideal in a Noetherian ring is the irredundant intersection of finitely many prime ideals and this is unique up to reordering. The Lasker-Noether theorem says that in a Noetherian ring any ideal can be written as an intersection of primary ideals. A proper ideal $\mathfrak{q} \subset A$ is primary, if in A/\mathfrak{q} every zero divisor is nilpotent. Equivalently, \mathfrak{q} is primary if $xy \in \mathfrak{q}$ implies $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. The Lasker-Noether theorem proven easily by combining the following two lemmata.

Lemma 7.1. *In a Noetherian ring, every ideal is an intersection of irreducible ideals.*

Here an ideal $I \in A$ is called **irreducible** if $I = J \cap K$ for ideals $J, K \subset A$ imply $I = J$ or $I = K$.

Proof. If nonempty, consider the set of ideals which cannot be written as an intersection of irreducible ideals. By Noetherian hypothesis, this set has a maximal element with respect to inclusion, call it I . I cannot be irreducible, therefore $I = J \cap K$ for some other ideals $J, K \supset I$. But then, J and K can be written as intersections of irreducible ideals, hence I can also which is a contradiction. \square

Lemma 7.2. *In a Noetherian ring, every irreducible ideal is primary.*

Proof. Let $\mathfrak{q} \subset A$ is an irreducible ideal. Consider $B = A/\mathfrak{q}$. Then (0) is irreducible and it suffices to show that (0) is primary in B . Let $x, y \in B$ such that $xy = 0$ and $x \neq 0$. Then $x \in \text{ann}(y)$. Consider the chain of ideals

$$\text{ann}(y) \subset \text{ann}(y^2) \subset \dots$$

By the Noetherian hypothesis, this chain stabilises. Thus, $\text{ann}(y^n) = \text{ann}(y^{n+1})$ for some $n > 0$. It follows that $(x) \cap (y^n) = (0)$. Indeed, if $b \in (x)$, then $by = 0$, and if $b \in (y^n)$ then $b = cy^n$ hence $by = cy^{n+1} = 0$ so $c \in \text{ann}(y^{n+1}) = \text{ann}(y^n)$. Hence $b = cy^n = 0$. Since (0) was assumed to be irreducible, and $x \neq 0$, we must have $(y^n) = (0)$, or $y^n = 0$ which proves (0) is primary. \square

The primary decomposition of a general ideal I is not as appealing as the prime ideal decomposition of a radical ideal as it need not be unique.

\triangleleft Let $A = k[x, y]$. Check that $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ are two distinct primary decomposition of (x^2, xy) .

However, if $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$ is an irredundant primary decomposition of I , then the minimal elements in the set $\{\sqrt{\mathfrak{q}_i} : i = 1, \dots, s\}$ give the minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ containing I that appear in the decomposition $\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_t$. Note that t can be smaller than s .

Homological methods. In multilinear algebra, given two A -modules M and N , one constructs a new A -module $M \otimes_A N$ called the tensor product of M and N over A . Moreover, if M and N are themselves rings B and C then the A -module $B \otimes_A C$ has a ring structure. A special case of this is when $A = k$, $B = k[V]$ and $C = k[W]$ are co-ordinate rings of varieties V and W , then $k[V] \otimes_k k[W]$ is the co-ordinate ring $k[V \times W]$ of the product $V \times W$. The study of tensor products involves short exact sequences, flat modules and the related notions which are covered in your Homological Algebra module (Algebra IV), hence this was left out here.

We have mostly covered what one might call the classical period of commutative algebra touching on important work of Hilbert, Noether, Krull which brings us up to roughly 1950s. Around this time, a kind of small revolution happens where homological algebra gets introduced in commutative algebra by Auslander and Buchsbaum, Northcott and Rees, and Serre. Some of these methods and results such as Serre's characterisation of regular local rings in terms of its homological dimension would be covered in a more advanced study of homological algebra.

Projective varieties and graded algebras. Projective varieties are compactifications of affine varieties obtained by taking the closure of an affine variety in the projective space $\mathbb{P}_k^n = k^n \cup \mathbb{P}_k^{n-1}$. Alternatively, they can be defined given as zero loci of homogeneous polynomials in the projective space \mathbb{P}_k^n . The algebraic counterpart of these are \mathbb{N} -graded rings, that is a decomposition of the form $A = A_0 \oplus A_1 \oplus \dots$ such that the multiplication respects the grading, that is $A_i A_j \subset A_{i+j}$. We leave this to your Algebraic Geometry module.

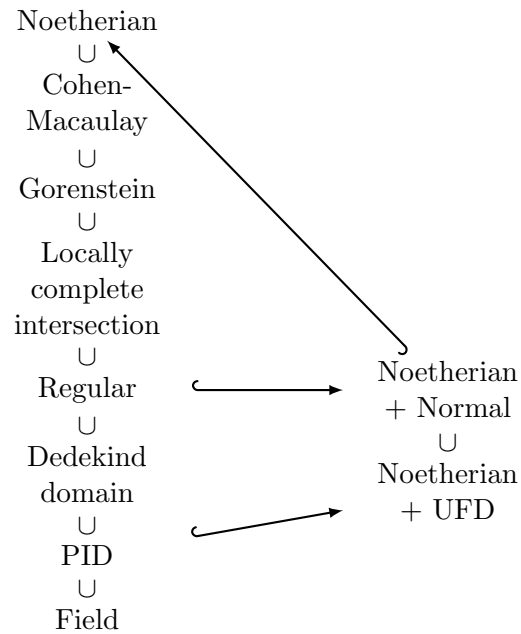
Schemes. We have discussed the (anti)equivalence of categories between finitely generated k -algebras and affine varieties (when k is algebraically closed.) In general, when we want to work with more general commutative rings (not necessarily including a field, or not necessarily nilpotent free), the notion of affine varieties have to be generalised to the notion of affine schemes. We have seen a first approximation to what affine schemes are by associating to an algebra A , its spectrum $\text{Spec}A$. However, what we are missing is the notion of a sheaf of rings which are thought of as functions on open sets of $\text{Spec}A$. Sheaves and schemes are usually introduced in a second course in Algebraic Geometry.

Dedekind domains and Ideal class group. We defined Dedekind domain and showed that every ideal in a Dedekind domain is a product of prime ideals, but we didn't prove the converse that says that if every ideal in an integral domain R is a product of prime ideals (in a unique way) then R is a Dedekind. The set of non-zero fractional ideals of a Dedekind domain form a free Abelian group with respect to multiplication. The quotient of this by principal fractional ideals is called the **ideal class group** of the Dedekind domain. This is a very important finite abelian group that is studied in your Algebraic Number Theory module.

Special classes of rings: Regular, Cohen-Macaulay, etc.

If R is a ring and M and R -module, a sequence x_1, \dots, x_r of elements of R is called a **regular sequence** for M if x_1 is not a zero-divisor in M and for all $i = 2, \dots, r$, x_i is not a zero divisor in $M/(x_1, \dots, x_{i-1})M$. If R is a local ring with maximal ideal \mathfrak{m} , then the **depth** of M is the maximum length of a regular sequence for M with all $x_i \in \mathfrak{m}$. We define $\text{depth}R$ by viewing R as an R -module. In a local Noetherian ring, one has $\text{depth}(\mathfrak{p}) \leq h(\mathfrak{p})$ for any prime ideal \mathfrak{p} . In particular, $\text{depth}R \leq \dim R$. A local Noetherian ring is called **Cohen-Macaulay** if $\text{depth}R = \dim R$. In a Cohen-Macaulay ring $\text{depth}(\mathfrak{p}) = h(\mathfrak{p})$ for any prime ideal \mathfrak{p} .

End of lec. 30



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] Kaplansky - Commutative Rings
- [6] Kunz - Introduction to Commutative Algebra and Algebraic Geometry
- [7] Schenk - Computational Algebraic Geometry
- [8] Arrondo - The Nullstellensatz without the Axiom of Choice. arXiv:2009.02837.