Math 902 Notes

Spring 2021

Contents

0 What is this course about? 2

1 Finiteness conditions 4
1.1 Finitely generated algebras and modules . . . 6
1.2 Integral extensions . . . 10
1.3 Noetherian rings and modules . . . 13
1.4 Application: invariant rings of finite groups . . . 17

2 Algebraic geometry 20
2.1 Affine algebraic sets and the Nullstellensatz . . . 20
2.2 The category of algebraic sets and algebraic morphisms . . . 30
2.3 The prime spectrum and the Zariski topology . . . 36

3 Primary decomposition 41
3.1 Primary ideals and primary decompositions . . . 42
3.2 Associated primes . . . 47
3.3 Interlude on localization . . . 50
3.4 Uniqueness aspects of primary decomposition . . . 55

4 Dimension theory I 58
4.1 Krull dimension . . . 59
4.2 Chains of primes in integral extensions . . . 63
4.3 Noether normalization and the dimension of affine domains . . . 68

5 Dimension theory II 72
5.1 Local rings and Nakayama's Lemma . . . 72
5.2 Artinian rings and finite length modules . . . 75
5.3 The Hilbert function of a graded algebra . . . 81
5.4 Associated graded rings, Hilbert-Samuel function . . . 86
5.5 The dimension theorem . . . 91
5.6 Regular local rings . . . 95

6 Where next? 99

Conventions

I am assuming knowledge of rings, modules and ideals at the level of a first year graduate course, e.g. UNL's Math 817–818. I will also assume knowledge of tensor products, localization, and some basic aspects of homological algebra.

This is a course in *commutative algebra*, so we stipulate that throughout the course

- all rings, unless specified otherwise, are commutative, unital, and nontrivial, meaning that $0 \neq 1$.
- all ideals I are assumed to be strict subsets of R. We will call R itself an improper ideal.
- all ring homomorphisms $R \to S$ are assumed to map $1_R \mapsto 1_S$

Chapter 0

What is this course about?

In 1637 Fermat attempted to solve the following equation in the integers:

$$x^n + y^n = z^n, \text{ where } n \geq 3 \text{ is an integer.}$$

A naive approach would be to factor this equation in the cyclotomic integers $\mathbb{Z}[\xi]$ as

$$\prod_{i=0}^{n-1}(x + \xi^{2i+1}y) = z^n, \text{ where } \xi \text{ is a primitive root of 1, } \xi^{2n} = 1$$

and try to identify the factors on both sides. But this is doomed to failure because $\mathbb{Z}[\xi]$ is not a UFD for $n \geq 23$. The realization of this problem prompted Dedekind to study factorization properties of rings and introduce the notion of ideals. Since factorizations of elements are only ever unique up multiplication by units, he wanted to study factorizations of ideals, e.g. (x^n+y^n), which are unchanged when the generator is multiplied by a unit. This marked the birth of commutative algebra.

What? In this course we study *commutative algebra*, i.e. the theory of commutative rings and the structure of their ideals and modules. The notion of localization of a ring is one of the main differences between commutative algebra and the theory of non-commutative rings. It leads to an important class of commutative rings, the local rings that have only one maximal ideal.

Why? Commutative algebra is essentially the study of the rings occurring in algebraic number theory, such as the cyclotomic integers, and algebraic geometry, such as the polynomial ring in several variables $\mathbb{C}[x_1, \ldots, x_n]$. We study it for its own sake in this class and explore the connections to group representation theory, algebraic geometry, and homological algebra.

Brief history (adapted from Wikipedia): The subject, first known as ideal theory, began with Richard Dedekind's work on ideals mentioned above. Later, David Hilbert

introduced the term ring to generalize the earlier term number ring. Hilbert introduced a more abstract approach to solve problems in classical invariant theory. In his 1890 paper he proved Hilbert's basis theorem, Hilbert's syzygy theorem, defined what we now call the Hilbert function and used these to prove finiteness for rings of invariants. In turn, Hilbert strongly influenced Emmy Noether, who recast many earlier results in terms of an ascending chain condition, now known as the noetherian condition. Another important milestone was the work of Hilbert's student Emanuel Lasker, who introduced primary decomposition.

The main figure responsible for the birth of commutative algebra as a mature subject was Wolfgang Krull, who introduced the fundamental notions of localization and completion of a ring, as well as that of regular local rings. He established the concept of the Krull dimension of a ring and his principal ideal theorem is widely considered one of the most important foundational theorems in commutative algebra. These results paved the way for the formalization of algebraic geometry through commutative algebra, an idea pioneered by Oscar Zariski and Alexandre Groethendieck, which would revolutionize the latter subject.

Chapter 1

Finiteness conditions

January 27, 2021

Here is some motivation from group representation theory which shows why finiteness conditions are desirable.

Recall that in representation theory, a group G acts on a finite dimensional vector space $V = K^n$ over a field K by linear transformations. We learned that the following are equivalent ways to describe such an action:

Definition 1.1. A K-linear action of G on $V = K^n$ can be defined by each of the following equivalent statements:

- $(v \mapsto g \cdot v) \in \mathrm{Aut}_K(V)$, $e \cdot v = v$, and $(gh)v = g(hv)$ for each $g, h \in G$ and $v \in V$
- $\rho : G \to \mathrm{Aut}_K(V) \cong GL_n(K)$ is a group homomorphism and $g \cdot v := \rho(g)(v)$
- V is a $K[G]$-module (recall that $K[G]$ is the group ring of G).

Now fix a basis for V, say $\{x_1, \ldots, x_n\}$ so that $V = \mathrm{Span}_K\{x_1, \ldots, x_n\}$. We will consider the polynomial ring $R = \mathrm{Sym}(V) = K[x_1, \ldots, x_n]$ generated by $\{x_1, \ldots, x_n\}$. Note that $V \subseteq R$ can be viewed as the set of homogeneous polynomials of degree one. We will extend the action of G from V to R in the following manner.

Lemma 1.2. *Let G be a group, K a field, $V = \mathrm{Span}_K\{x_1, \ldots, x_n\}$ a finite dimensional vector space, and $R = K[x_1, \ldots, x_n]$. Any K-linear group action $\rho : G \to \mathrm{Aut}_K(V)$ induces a group homomorphism*

$$\Phi : G \to \mathrm{Aut}_{ring}(R), \qquad \Phi(g)(f(x_1, \ldots, x_n)) = f(g \cdot x_1, \ldots, g \cdot x_n).$$

Proof. One needs to show for well definedness that $\Phi(g)$ is a ring automorphism. Using g^{-1} in the definition of Φ (rather than g) is needed for proving that Φ is a group homomorphism:

$$\begin{aligned} \Phi(gh)(f(x_1, \ldots, x_n)) &= f((gh) \cdot x_1, \ldots, (gh) \cdot x_n) \\ &= f(g(h \cdot x_1), \ldots, g(h \cdot x_n)) \\ &= \Phi(g) f(h \cdot x_1, \ldots, h \cdot x_n) \\ &= \Phi(g)\Phi(h)(f(x_1, \ldots, x_n)). \end{aligned}$$

One also needs to show Φ is a group homorphism. I leave both tasks as exercise. $\square$

Remark 1.3. Note that $R = K[x_1, \ldots, x_n]$ is an (infinite dimensional) K vector space. The map Φ above is in fact K-linear because it commutes with multiplication and $\Phi(k) = k$ for each constant polynomial $k \in K$. Therefore we can also view it as a group homomorphism

$$\Phi : G \to \mathrm{Aut}_K(R)$$

which makes R into an (infinite dimensional) K-linear representation of G.

Notation 1.4. We denote the action of G on R in Lemma 1.2 above by

$$g \cdot f(x_1, \ldots, x_n) = f(g \cdot x_1, \ldots, g \cdot x_n). \tag{1.1}$$

This determines a subring of R.

Definition 1.5. For any K-algebra R and any group G of K-linear automorphisms of R define the *ring of invariants* with respect to the action of G on R to be

$$R^G = \{f \in R \mid g \cdot f = f \text{ for all } g \in G\}.$$

Example 1.6. Let S_n be the symmetric group on n letters acting on $R = K[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$. Then

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

If $n = 3$, then $f = x_1^2 + x_2^2 + x_3^2$ is invariant, while $g = x_1^2 + x_1x_2 + x_2^2 + x_3^2$ is not, since swapping 1 with 3 gives a different polynomial.

How many invariant polynomials are there? It is easy to see that there are infinitely many, for example $f_d = x_1^d + x_2^d + \cdots x_n^d$ is invariant for any $d \in \mathbb{N}$. However, the *Fundamental Theorem of Symmetric Polynomials* (FTSP) says that every element of R^{S_n} can be written in terms of finitely many invariant polynomials called fundamental invariants.

Theorem 1.7 (Fundamental theorem of Symmetric Polynomials = FTSP)**.** *If $R = K[x_1, \ldots, x_n]$, every symmetric polynomial in R, i.e., every element of R^{S_n} can be written as polynomial expression in the elementary symmetric polynomials*

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

In symbols, FTSP says that $R^{S_n} = K[e_1, \ldots, e_n]$.

For a concrete example, f above is

$$f = e_1^2 - 2e_2 = P(e_1, e_2, e_3), \text{ where } P(y_1, y-2, y_3) = y_1^2 - y_2.$$

FTSP says that a set of fundamental invariants of the symmetric group are the elementary symmetric polynomials $e_1, \ldots, e_n$ listed above. Another set of fundamental invariants of the symmetric group are the polynomials $f_j = \sum_{i1=}^{n} x_i^j$ with $1 \leq j \leq n$.

Question 1.8 (Finite generation problem for rings of polynomial invariants)**.** *If G is a group acting K-linearly on $R = K[x_1, \ldots, x_n]$ as in (1.1), is there always a finite set of invariant polynomials $f_1, \ldots, f_t$ (such that every element of R^G can be expressed as a polynomial expression in terms of them, i.e. $R^G = K[f_1, \ldots, f_t]$?*

We will answer this question in the affirmative for finite groups, under mild conditions on $\mathrm{char}(K)$, as Hilbert and Noether did, by the end of the chapter.

1.1 Finitely generated algebras and modules

January 29, 2021

1.1.1 Finitely generated algebras

Definition 1.9 (Algebra)**.** Given a ring A, an A-algebra is a ring R equipped with a ring homomorphism $\varphi : A \to R$ called the *structure map*. (If R is not assumed commutative we require the image of φ to be contained in the center of R.) This defines an A-module structure on R given by restriction of scalars, that is, for $a \in A$ and $r \in R$, $ar := \varphi(a)r$ which is compatible with the internal multiplication of R i.e

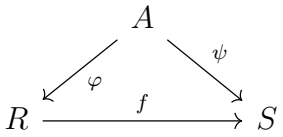
$$a(rs) = (ar)s = r(as) \text{ for all } a \in A, rs \in R.$$

Remark 1.10. The definition above only depends on the image of φ, which is a subring $A' = \varphi(A) \subseteq R$. The A-algebra structure of R is the same as its A' algebra structure with structural map given by the inclusion $A' \hookrightarrow R$. So we will usually assume, unless specified otherwise, that $A \subseteq R$ and $\varphi = A \hookrightarrow R$. In this case the A-module multiplication ar coincides with the internal (ring) multiplication on R.

Example 1.11.

- $A \hookrightarrow A[x_1, \ldots, x_n]$ makes the polynomial ring into an A-algebra called *the free A-algebra* on $\{x_1, \ldots, x_n\}$
- $M_n(A)$ is a (non-commutative) A-algebra w.r.t $\varphi : M_n(A) \to A, a \mapsto aI_n$

Definition 1.12. An *A-algebra homomorphism* between A-algebras R, S with structure maps $\varphi : A \to R$ and $\psi : A \to S$ is a ring homomorphism $f : R \to S$ that makes the following diagram commute



Exercise 1.13. Show that

$$\mathrm{Hom}_{A-alg}(R,S) = \mathrm{Hom}_{A-mod}(R,S) \cap \mathrm{Hom}_{rings}(R,S)$$

Proposition 1.14. *The collection of A-algebras and A-algebra homomorphisms forms a category denoted $\langle\langle A\text{-}Algebras\rangle\rangle$.*

Definition 1.15 (Algebra generation)**.** Let R be an A-algebra with structure map $\varphi : A \to R$ and let $\Lambda \subseteq R$ be a set. The *A-subalgebra* of R *generated by* Λ, denoted $A[\Lambda]$, is the smallest (w.r.t containment) subring of R containing Λ and $\varphi(A)$.

A set of elements $\Lambda \subseteq R$ *generates* R as an A-algebra if $R = A[\Lambda]$.

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

Lemma 1.16. *The following are equivalent:*

1. *Λ generates R as an A-algebra, i.e. $R = A[\Lambda]$.*
2. *Every element in R admits a polynomial expression in Λ with coefficients in $\varphi(A)$, i.e.*
$$R = \left\{ \sum_{finite} \varphi(a)\lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N} \right\}.$$
3. *The ring homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on a set of indeterminates X, $\psi|_X$ maps X to Λ bijectively and $\psi|_A = \varphi$ (the structure map), is surjective.*

Proof. I will only sketch (1) $\Rightarrow$ (2). Consider the set

$$S = \left\{ \sum_{finite} \varphi(a)\lambda_1^{i_1} \cdots \lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N} \right\}.$$

It is easy to check that this is a subring of R and that it contains Λ and A. Thus $A[\Lambda] \subseteq S$ by the definition of $A[\Lambda]$. Since $A[\Lambda] = R$ it follows that $A[\Lambda] = S = R$.

For (2) $\Rightarrow$ (3) note that $S = \mathrm{Im}(\psi)$. □

Exercise 1.17. Prove Lemma 1.16.

Note that the homomorphism in part (3) need nor be injective.

Definition 1.18. If the homomorphism ψ is injective (so an isomorphism) we say that $R \cong A[X]$ is a *free* A-algebra. The set $\mathrm{Ker}(\psi)$ measures how far R is from being a free A-algebra and is called the set of *relations* of R.

We say that a set of elements $X = \{r_1, \ldots, r_n\}$ of R are *algebraically independent* over A if the algebra $A[r_1, \ldots, r_n]$ is a free A-algebra. Equivalently, this means that no polynomial expression with coefficients in A and "variables" $r_1, \ldots, r_n$ is 0 in R.

Definition 1.19 (Algebra-finite)**.** We say that a ring homomorphism $\varphi : A \to R$ is *algebra-finite*, or R is a *finitely generated A-algebra*, if there exists a *finite* set Λ that generates R as an A-algebra, i.e. $R = A[\Lambda]$.

The term *finite-type* is also used with the same meaning (but I will not use it).

Corollary 1.20. *Every finitely generated A-algebra is a quotient of a finitely generated free A-algebra.*

Proof. Follows from part (3) of Lemma 1.16. □

Example 1.21. The ring $K[x_1, \ldots, x_n]^{S_n}$ of Example 1.6 is generated by $\{e_1, \ldots, e_n\}$ as a K-algebra. In fact in this case $K[x_1, \ldots, x_n]^{S_n} = K[e_1, \ldots, e_n]$ is a free K-algebra (there are no relations between the elementary symmetric polynomials)

Example 1.22. The ring $\mathrm{M}_n(A)$ is generated by $\Lambda = \{E_{ij} \mid 1 \leq i, j \leq n\}$ as an A-algebra, where E_{ij} has 1 in position ij and 0 elsewhere. However in this case there are relations $E_{ij}E_{kl} = \delta_{jk}E_{il}$ between the generators.

Example 1.23. Let $A = K$ be a field, and $B = K[x, xy, xy^2, xy^3, \cdots] \subseteq C = K[x, y]$, where x and y are indeterminates. Any finitely generated subalgebra of B is contained in $K[x, xy, \ldots, xy^m]$ for some m, since we can write the elements in any finite generating set as polynomial expressions in the finitely many specified generators of B. But, every element of $K[x, xy, \ldots, xy^m]$ is a K-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated A-algebra even though C is.

Proposition 1.24 (Transitivity for algebra-finite)**.** *Let $A \subseteq B \subseteq C$ be rings. Then:*

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

More generally, for ring homomorphisms φ, ψ

- *$\varphi : A \to B, \psi : B \to C$ algebra-finite $\implies$ $\psi \circ \varphi : A \to C$ is algebra-finite.*

Exercise 1.25. Prove Proposition 1.24.

Remark 1.26.

1. Any surjective ring homomorphism $\varphi : A \to R$ is algebra-finite: the target is generated by 1_R.
2. Since any homomorphism $\phi : A \to R$ can be factored as $\phi = \psi \circ \varphi$ where φ is the surjection $\varphi : A \to A/\operatorname{Ker}(\varphi)$ and ψ is the inclusion $\psi : A/\operatorname{Ker}(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms by the last bullet point of Proposition 1.24.

February 1, 2021

1.1.2 Finitely generated modules

We will also find it quite useful to consider a stronger finiteness property for rings/maps.

Definition 1.27. (Module generation) Let M be an A-module and let $\Gamma \subseteq M$ be a set. The *A-submodule of M generated by Γ*, denoted $\sum_{\gamma\in\Gamma} A\gamma$, is the smallest (w.r.t containment) submodule of M containing Γ.

A set of elements $\Gamma \subseteq M$ *generates* M as an A-module if the submodule of M generated by Γ is M itself, i.e. $M = \sum_{\gamma\in\Gamma} A\gamma$.

This also has some equivalent realizations:

Lemma 1.28. *The following are equivalent*

1. *Γ generates M as an A-module.*
2. *Every element of M admits a linear combination expression in the elements of Γ with coefficients in A, that is*
$$M = \left\{ \sum_{i=1}^{n} a_i\gamma_i \mid a_i \in A, \gamma_i \in \Gamma, n \in \mathbb{N} \right\}.$$
3. *The homomorphism $\theta : A^{\oplus Y} \to M$, where $A^{\oplus Y} = \bigoplus_{y\in Y} Ay$ is a free A-module with basis Y and $\theta|_Y$ maps Y to Γ bijectively, is surjective.*

If the map θ is injective, M is called a *free* A-module and Γ is called a *basis* of M. The kernel of the homomorphism in part (3) is called the set of *syzygies* on Γ.

Exercise 1.29. Prove Lemma 1.28.

Definition 1.30 (Module-finite)**.** An A-module M is said to be finitely generated if there exists finite set Γ such that $M = \sum_{\gamma\in\Gamma} A\gamma$.

A ring homomorphism $\varphi : A \to R$ is *module-finite* if R is a *finitely-generated A-module*.

The following follows from part (3) of Lemma 1.28.

Corollary 1.31. *Every finitely generated A-module is a quotient of A^n for some $n \in \mathbb{N}$.*

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

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

Lemma 1.32 (Module-finite $\Rightarrow$ algebra-finite)**.** *If $\varphi : A \to R$ is module-finite then it is algebra-finite. The converse is not necessarily true.*

Example 1.33. 1. If $K \subseteq L$ are fields, L is module-finite over K just means that L is a finite field extension of K.

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

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

Exercise 1.34. Show that the inclusion of $K[x] \subseteq K[x, 1/x]$ is not module-finite.

As with the algebra-finite property, we have:

Proposition 1.35 (Transitivity for module-finite)**.** *Let $A \subseteq B \subseteq C$ be rings. Then*

- *$A \subseteq B$ module-finite and $B \subseteq C$ module-finite $\implies$ $A \subseteq C$ module-finite, and*
- *$A \subseteq C$ module-finite $\implies$ $B \subseteq C$ module-finite,*
- *but again, $A \subseteq C$ module-finite $\not\implies$ $A \subseteq B$ module-finite.*

Proposition 1.36. *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of modules.*

- *If M', M'' are finitely generated, then M is finitely generated.*
- *If M is finitely generated, then M'' is finitely generated.*
- *If M is finitely generated then M' need not be finitely generated.*

Exercise 1.37. Prove Propositions 1.35 and 1.36.

For counterexamples relevant to the third bullet points in the above propositions see problem 5 on homework 1.

1.2 Integral extensions

We have seen that a module-finite inclusion of fields is just a finite field extensions. Recall that finite field extensions are algebraic. Now we introduce a similar concept to being an algebraic element but for rings instead of fields.

Definition 1.38 (Integral element/extension)**.** Let $\varphi : A \to R$ be a ring homomorphism and $r \in R$. The element $r \in R$ is *integral* over A if there are elements $a_0, \dots, a_{n-1} \in A$ such that

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

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

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

If $A \subseteq R$, the *integral closure of A in R* is the set of elements of R that are integral over A. The integral closure of a domain A in its fraction field is usually denoted $\overline{A}$.

Evidently, an integral extension of fields is the same as an algebraic field extension, but the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings.

Example 1.39. What is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$?

If $r = p/q$ satisfies the equation in the definition of integral element, then $p \mid a_0$ and $q \mid 1$ so $r \in \mathbb{Z}$. Conversely, every element of $\mathbb{Z}$ is integral over $\mathbb{Z}$, so the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

Exercise 1.40. The ring $\mathbb{Z}[d] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is integral over $\mathbb{Z}$.

The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Like our other types of ring maps, we see that $r \in R$ is integral over A if and only if r is integral over the subring $\varphi(A) \subseteq R$, so we can restrict our focus to inclusion maps $A \subseteq R$.

February 3, 2021

Proposition 1.41. *Let $A \subseteq R$ be rings.*

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

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

2. Write $A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \ldots, r_t]$. Note that r_i is integral over A_{i-1}: use the same monic equation of r_i over A. Then, the inclusion $A \subseteq A[r_1, \ldots, r_t]$ is a composition of module-finite maps, hence is module-finite. □

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

Next we want to make precise the relationship between integral and module-finite.

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

Lemma 1.42 (Determinant trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^n$, and $r \in R$.*

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

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

The ring R is a $\mathbb{Z}$-algebra (every ring is a $\mathbb{Z}$-algebra, but generally not finitely generated as such), so we can write R as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \to R$ be a surjection, let $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that $\psi(\mathrm{adj}(A)_{ij}) = \mathrm{adj}(B)_{ij}$ and $\psi((\mathrm{adj}(A)A)_{ij}) = (\mathrm{adj}(B)B)_{ij}$, since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish the lemma in the case $R = \mathbb{Z}[X]$. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of its fraction field. Since both sides of the equation live in R and are equal in the fraction field (by linear algebra) they are equal in R.

2. We have $(rI_{n\times n} - B)v = 0$, so $\det(rI_{n\times n} - B)v = \mathrm{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0$. □

Theorem 1.43 (Module finite implies integral)**.** *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

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

Write $R = \sum_{i=1}^{t} Ar_i$. We may assume that $r_1 = 1$, since we can always enlarge a set of module generators. By assumption, we can find $a_{ij} \in A$ such that

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

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

Theorem 1.44 (Module-finite = algebra-finite + integral)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): This direction follows from Lemma 1.32 and Theorem 1.43.

($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.41. □

Corollary 1.45. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the integral closure of A in S forms a subring of S.*

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

For the latter statement,

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

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

Exercise 1.46 (Integral localizes)**.** Let $A \subseteq R$ be rings and $S \subseteq A$ a multiplicatively closed set. If $A \subseteq R$ is integral then $S^{-1}A \subseteq S^{-1}R$ is integral.

1.3 Noetherian rings and modules

You might recall the notion of noetherian rings form Math 817–818 where it was proved that finite factorizations into irreducible elements exist in noetherian rings.

Definition 1.47 (noetherian ring)**.** A ring R is *noetherian* if for every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ there is some N so that $I_n = I_{n+1}$ for all $n > N$. If this is the case, we say that the chain eventually stabilizes.

This condition also admits some equivalences.

Proposition 1.48 (Equivalences for noetherian ring)**.** *The following are equivalent for a ring R.*

1. *R is a noetherian ring.*
2. *Every nonempty family of ideals has a maximal element (under containment).*
3. *Every ascending chain of finitely generated ideals of R eventually stabilizes.*
4. *Every ideal of R is finitely generated.*

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

(2)⇒(3): Think of a the elements of an ascending chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals as a family of ideals. If I_N is a maximal element of this family then $I_N = I_n$ for all $n \geq N$ by the definition of maximal.

(3)⇒(4): We prove the contrapositive. Suppose that there is an ideal I such that no finite subset of I generates I. For any finite $S \subseteq I$ we have $(S) \subsetneq I$, so there is some $s \in I \setminus (S)$. Thus, $(S) \subsetneq (S \cup \{s\})$. Inductively, we can continue this to obtain an infinite proper chain of finitely generated ideals, contradicting (3).

(4)⇒(1): Given an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ let $I = \bigcup_{n\in\mathbb{N}} I_n$. The ideal I is finitely generated, say $I = (a_1, \ldots, a_t)$, and since each a_i is in some I_{n_i}, there is an N such that each a_i is in I_N. But then $I_n = I = I_N$ for all $n > N$. □

Example 1.49. 1. Any field is noetherian: the only ideals are (0) and (1).

2. If R is a PID, then R is noetherian: every ideal is finitely generated.

3. A ring that is *not* noetherian is a polynomial ring in infinitely many variables $K[x_1, x_2, \ldots]$: the ascending chain of ideals $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ does not stabilize.

   Note: a subring of a noetherian ring need not be noetherian. $K[x_1, x_2, \ldots]$ is a subring of its fraction field which is a noetherian ring by (1).

4. Another ring that is *not* noetherian is the ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots]$ A nice ascending chain of ideals is

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

   This is also a non-noetherian subring of a noetherian ring, namely $\overline{K[x]}$ the integral closure of $K[x]$ in its fraction field.

We can get new noetherian rings from old by quotienting.

Remark 1.50. If R is a noetherian ring, and I is an ideal of R, then R/I is a noetherian ring as well since there is an order-preserving bijection

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

Definition 1.51 (Noetherian module)**.** An R-module M is *noetherian* if every ascending chain of submodules of M, $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$, eventually stabilizes.

Example 1.52. If R is a noetherian ring then R is also a noetherian R-module. However **a noetherian ring need not be a noetherian module over a subring.** For example, consider $\mathbb{Z} \subseteq \mathbb{Q}$. These are both noetherian (as rings) by $\mathbb{Q}$ is not a noetherian $\mathbb{Z}$-module because it has an ascending sequence of submodules which does not stabilize

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

There are analogous criteria for modules to (1)–(4) above namely:

Proposition 1.53 (Equivalences for noetherian module)**.** *The following are equivalent for a module M:*

1. *M is a noetherian module.*
2. *Every nonempty family of submodules has a maximal element.*
3. *Every ascending chain of finitely generated submodules of M eventually stabilizes.*
4. *Every submodule of M is finitely generated.*

In particular, a noetherian module must be finitely generated.

Exercise 1.54. Prove the above proposition.

Remark 1.55. Condition (2) of Propositions 1.48 and 1.53 allows us to avoid using Zorn's Lemma. So noetherianity is able to bypass any logical controversy.

Lemma 1.56 (Noetherianity in exact sequences)**.** *In an exact sequence of modules*

$$0 \to N \to M \to L \to 0$$

M is noetherian if and only if N and L are noetherian.

Proof. Homework 1 problem 4. □

Corollary 1.57. *A module M is noetherian if and only if $M^n = \bigoplus_{i=1}^n M$ is noetherian. In particular, if R is a noetherian ring then R^n is a noetherian module for $n \in \mathbb{N}$.*

Proof. By induction on n:

- the case $n = 1$ is a tautology
- for $n > 1$ consider the short exact sequence

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

and apply Lemma 1.56 and the inductive hypothesis to get the desired conclusion.

□

Next we see that over noetherian rings the noetherian property for modules is equivalent to the module-finite condition.

Proposition 1.58. *Let R be a noetherian ring. Then M is a noetherian module if and only if M is finitely generated.*

Proof. If M is noetherian, it (and all of its submodules) is finitely generated by the equivalences in Proposition 1.53.

Now let R be noetherian and M be f.g.. By the Corollary above the free module $R^n = \bigoplus_{i=1}^n Re_i$ is noetherian for all $n \in \mathbb{N}$. Now, a finitely generated module M is quotient of a finitely generated free module, R^n, so is noetherian by Lemma 1.56. □

This has two interesting corollaries that I will leave as exercises.

Corollary 1.59.
1. *If R is noetherian, then any submodule of a finitely generated R-module is also a finitely generated module.*
2. *If A is noetherian and $A \subseteq R$ is module-finite then R is a noetherian ring.*

In fact a stronger statement is true: for an extension of a noetherian ring the algebra-finite condition is sufficient to imply the noetherian property for the extension. This will be the contents of Hilbert's basis theorem, Theorem 1.61. This was proven by Hilbert in 1890.

Definition 1.60. If R is a commutative ring and x is an indeterminate the set

$$R[[x]] = \left\{ \sum_{i \geq 0} r_i x^i \mid r_i \in R \right\}$$

with the obvious addition and multiplication is called the *(formal) power series ring* in the variable x with coefficients in R.

If $x_1, \ldots, x_d$ are distinct indeterminates the *(formal) power series ring* in all of these variables is defined inductively as

$$R[[x_1, \ldots, x_n]] = (R[[x_1, \ldots, x_{d-1}]])\,[[x_d]].$$

Theorem 1.61 (Hilbert Basis Theorem = HBT)**.** *Let A be a noetherian ring and let $x_1, \ldots, x_d$ be indeterminates. Then $A[x_1, \ldots, x_d]$ and $A[\![x_1, \ldots, x_d]\!]$ are noetherian.*

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

By induction on d, we reduce to the case $d = 1$. So we wish to show that A noetherian implies that $A[x]$ is a noetherian ring.

For $f \in A[x]$ define the leading coefficient of f to be the unique element $\mathrm{lc}(f) \in A$ such that

$$f = \mathrm{lc}(f)x^{\deg(f)} + \text{ lower degree terms}$$

Let $I \subseteq A[x]$ be an ideal and let

$$J = \{\mathrm{lc}(f) \mid f \in I\}.$$

Then J is easily seen to be an ideal of A, which is finitely generated because of the noetherian hypothesis on A. Let $J = (a_1, \ldots, a_t)$. Pick $f_1, \ldots, f_t \in A[x]$ such that the leading coefficient of f_i is a_i and set $N = \max_i\{\deg f_i\}$.

Claim: Every $f \in I$ can be written as $f = g + h$ with $g \in I \cap \sum_{i=0}^{N} Ax^i$ and $h \in (f_1, \ldots, f_t)$.

Proof of claim: The proof is by induction on $\deg(f)$.

Base case: if $\deg(f) \leq N$ then take $g = f, h = 0$.

Inductive step: assume that $\deg(f) > N$ and that every element of I of degree strictly smaller than $\deg(f)$ can be written as in the claim. Now $\mathrm{lc}(f) \in J$, hence $\mathrm{lc}(f) = \sum_{i=1}^{t} a_i b_i$ for some $b_i \in A$. Thus we can cancel off the leading term of f by subtracting a suitable linear combination of the f_is. Specifically the polynomial $f' = f - \sum_{i=1}^{t} b_i f_i x^{\deg(f)-\deg(f_i)}$ has degree strictly less than $\deg(f)$. By the inductive

hypothesis $f' = g' + h'$ with $g' \in I \cap \sum_{i=0}^{N} Ax^i$ and $h' \in (f_1, \ldots, f_t)$. Setting $g = g'$ and $h = h' + b_i f_i x^{\deg(f)-\deg(f_i)}$ proves the claim. □

Since A is noetherian and $I \cap \sum_{i=0}^{N} Ax^i$ is a submodule of a finitely generated free A-module, it is also finitely generated as an A-module (see Corollary 1.59), say by $\{f_{t+1}, \ldots, f_s\}$.

Then $I = (f_1, \ldots, f_t, f_{t+1}, \ldots, f_s)$ since if $f = g + h$ as in the claim we can write g as an A-linear (hence also $A[x]$-linear) combination of $f_{t+1}, \ldots, f_s$ and we can write h as an $A[x]$-linear combination of $f_1, \ldots, f_t$.

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

Corollary 1.62. *If A is a noetherian ring, then any finitely generated A-algebra is noetherian. In particular, any finitely generated algebra over a field is noetherian.*

Proof. Any finitely generated A-algebra is a quotient of a free finitely generated A-algebra by Lemma 1.16. By HBT, since A is a noetherian ring, any free finitely generated A-algebra is noetherian. By Remark 1.50 it follows that R is a noetherian ring. □

Remark 1.63. The converse of this Corollary is false.

1.4 Application: invariant rings of finite groups

We now want to move towards answering our Question 1.8 using our various notions of finiteness.

Theorem 1.64 (Noether's theorem on finite generation for rings of invariants)**.** *Let K be a field and R a finitely generated K-algebra. Let G be a finite group acting K-linearly on R, i.e. there is a group homomorphism $\Theta : G \to \mathrm{Aut}_{\langle\langle K\text{-algebras}\rangle\rangle}(R)$.*

Then R^G is a finitely generated K-algebra.

Proof. Let $R = K[u_1, \ldots, u_d]$, let t be an indeterminate and let $r = |G|$. Extend the action of G to $R[t]$ by letting $g \cdot t = t$ for all $g \in G$. Consider for $1 \leq i \leq d$ the polynomials

$$f_i = \prod_{g \in G} (t - gu_i) = t^r + c_{i,r-1}t^{r-1} + \cdots + c_{i,1}t + c_{i,0} \in A[t]$$

and notice that $g(f_i) = f_i$ for all $g \in G$, thus $c_{i,j} \in R^G$ for all i, j.
The ring $S = K[c_{ij}]_{1 \leq i \leq d, 0 \leq j \leq r}$ is noetherian by HBT since it is a finitely generated K-algebra.

In the extension tower

$$K \subseteq S \subseteq R^G \subseteq R$$

we have

- $S \subseteq R = S[u_1, \ldots, u_n]$ is module-finite by Proposition 1.41 because each u_i is integral over S
- Since $S \subseteq R$ is module-finite $S \subseteq R^G$ is also module-finite by Corollary 1.59
- since $K \subseteq S$ and $S \subseteq R^G$ are algebra-finite (the latter is even module-finite), then $K \subseteq R^G$ is algebra-finite by transitivity.

□

The history is a follows: Hilbert, in his famous 1980 paper, gave a proof that for $G = \mathrm{SL}_n(\mathbb{C})$, the ring of invariants of G acting on the ring of polynomials $R = \mathbb{C}[x_1, \ldots, x_n]$ is finitely generated. I will include a problem on homework set 2 that uses some of the same technique Hilbert used.

His proof goes as follows:

- show that R^G is a direct summand of R by constructing an analogue of the Reynolds operator (This step is tricky; I won't give details on why it works.)
- apply Hilbert's basis theorem to see that R is a Noetherian ring (this is why Hilbert proved that theorem)
- apply the homework problem that states direct summands of noetherian rings are noetherian to conclude R^G is a noetherian ring
- let I be the ideal of R^G generated by the elements of R^G of positive degrees
- then I has a finite set of generators $f_1, \ldots, f_t$ which can be chosen to be homogeneous
- finally, show that $R^G = \mathbb{C}[f_1, \ldots, f_t]$

Of course, the notion of noetherian ring had not been invented in 1890. Emmy Noether's contribution was to recognize that this notion is the key to the proof above. Defining and studying this notion, she was able to generalize Hilbert's proof to any R and finite G as shown in Theorem 1.64. Noetherian rings are named in her honor.

Remark 1.65. Note that the proof of Theorem 1.64 as well as Hilbert's proof are non-constructive as they do not give an explicit set of algebra generators for R^G invariants. Finding such a set of fundamental invariants for a given group is a difficult problem.

February 10, 2020

Now, we prove a technical theorem that relates all our finiteness notions. The statement is a bit complicated, but the result will be pretty useful.

Theorem 1.66 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

- *A is noetherian,*
- *C is module-finite over B or C is integral over B, and*
- *C is algebra-finite over A.*

Then, B is algebra-finite over A.

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

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

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

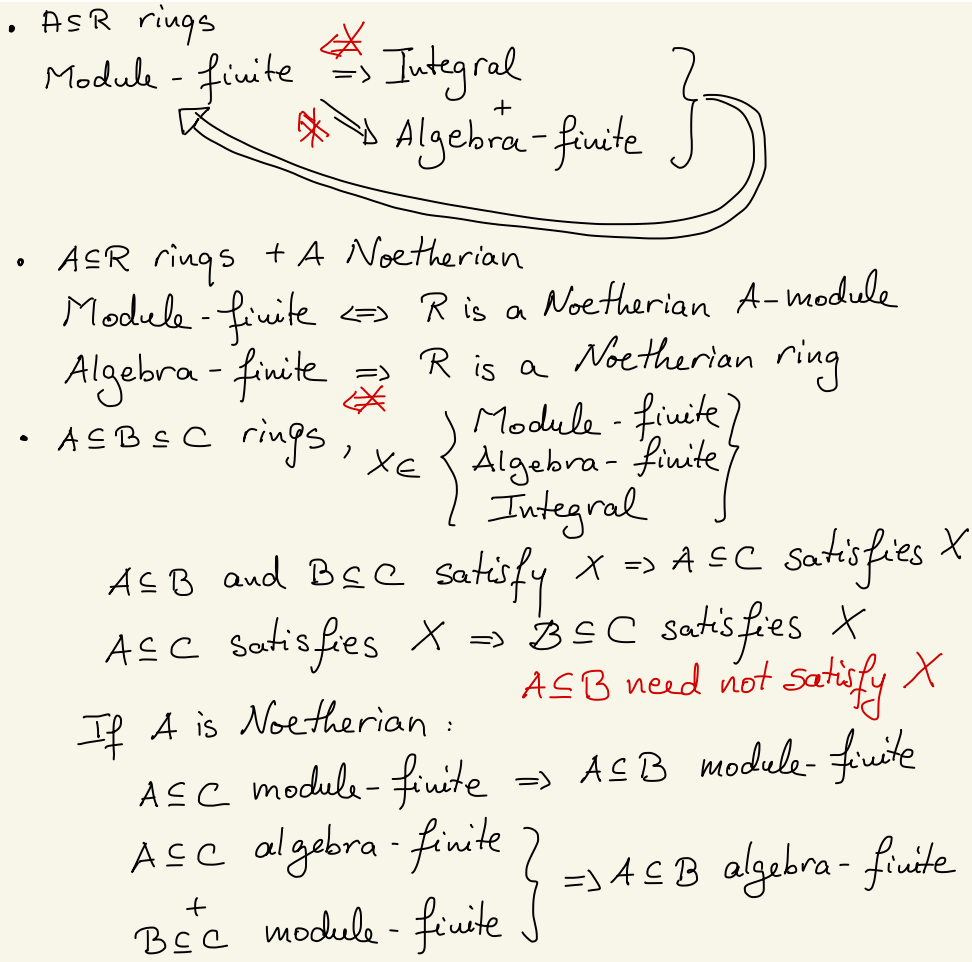
We claim that $C = \sum_{i=1}^{s} B_0\, g_i$. Given an element $c \in C$, write c as a polynomial expression in $\underline{f}$, hence we have that $c \in A[\{b_{ij}\}][g_1, \ldots, g_s]$. Then, using the equations for $g_i g_j$, we can write c in terms of just B_0-linear combinations of the g_i as required.

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

With this we can give a different proof of Noether's theorem.

Second proof of Noether's Theorem. Observe that $K \subseteq R^G \subseteq R$, that K is noetherian, $K \subseteq R$ is algebra-finite, and $R^G \subseteq R$ is module-finite because it is algebra-finite and integral as in the first proof. Thus, by the Artin-Tate Lemma, we are done! □

Here is a summary for the chapter



Chapter 2

Algebraic geometry

A motivating question to lead us to our next big theorem is the following:

Question 2.1. *To what extent is a system of polynomial equations*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_t(x_1, \ldots, x_n) = 0 \end{cases}$$

with $f_1, \ldots, f_t \in K[x_1, \ldots x_n]$ determined by its solution set?

Let's consider one polynomial equation in one variable. Over $\mathbb{R}, \mathbb{Q}$, or other fields that aren't algebraically closed, there are many polynomials with an empty solution set. On the other hand, over $\mathbb{C}$, or any algebraically closed field, if $f(z) = 0$ has solutions $z_1, \ldots, z_d$, we know that $f(z) = \alpha(z - z_1)^{a_1} \cdots (z - z_d)^{a_d}$, so that f is determined up to scalar multiple and repeated factors. Note that if we insists that f has no repeated factors, i.e. $a_i = 1$ for all i, then f is determined up to scalar multiple. Another way to say this is that the ideal (f) is uniquely determined by $z_1, \ldots, z_d$, if we insist that f does not have repeated factors.

More generally, given any system of polynomial equations $f_1 = \cdots = f_t = 0$, where $f_i \in K[z]$ for some field K, notice that that $z = a$ is a solution if and only if it is a solution for any polynomial $g \in (f_1, \ldots, f_t)$. But since $K[z]$ is a UFD, we have $(f_1, \ldots, f_t) = (f)$, where f is a GCD of $f_1, \ldots, f_t$ and so $z = a$ is a solution to the system if and only if $f(a) = 0$.

We will move on to polynomial equations in (finitely) many variables next.

2.1 Affine algebraic sets and the Nullstellensatz

Definition 2.2. For a field K the *affine n-space over K* denoted $\mathbb{A}^n_K$ is the set of n-tuples of elements of K

$$\mathbb{A}^n_K = \{(a_1, \ldots, a_n) \mid a_i \in K\}.$$

2.1.1 Points and maximal ideals

We will prove the following correspondence, which can be considered as an algebraic description of affine space:

Theorem 2.3. *If K is an algebraically closed field, then every maximal ideal of $K[x_1, \ldots, x_n]$ has the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some elements $a_1, \ldots, a_n \in K$ and the function*

$$\mathbb{A}^n_K \to \{\textit{maximal ideals of } K[x_1, \ldots, x_n]\},$$
$$(a_1, \ldots a_n) \mapsto (x_1 - a_1, \ldots, x_n - a_n)$$

is bijective.

To prove this we need to go over some notions of field theory.

Definition 2.4. Let $K \subseteq L$ be an extension of fields. A *transcendence basis* for L over K is a maximal algebraically independent subset of L.

Remark 2.5.

1. Every field extension has a transcendence basis. This is given by Zorn's Lemma once we see that a union of an increasing chain of algebraically independent sets is algebraically independent. Indeed if there were a nontrivial relation on some elements in the union, there would be a nontrivial relation on finitely many, and so a relation in one of the members in the chain.

2. Every set of field generators for L/K contains a transcendence basis. This is also given by Zorn's lemma considering algebraically independent subsets of the given generating set.

3. Observe that $\{x_\lambda\}_{\lambda \in \Lambda}$ is a transcendence basis for L over K, if an only if there is a factorization
$$K \subseteq K(\{x_\lambda\}_{\lambda \in \Lambda}) \subseteq L$$
where the first inclusion is *purely transcendental*, or isomorphic to a field of rational functions, and the second inclusion is algebraic (integral). If the latter were not algebraic, there would be an element of L transcendental over $K(\{x_\lambda\}_{\lambda \in \Lambda})$, and we could use that element to get a larger algebraically independent subset, contradicting the definition of transcendence basis. Conversely, if $K \subseteq K(\{x_\lambda\}_{\lambda \in \Lambda}) \subseteq L$ with the first inclusion purely transcendental and the second algebraic, $\{x_\lambda\}_{\lambda \in \Lambda}$ is a transcendence basis.

February 12, 2021

Here is a fact we will use later, whose proof we omit.

Theorem 2.6. *Let $K \subseteq L$ be an extension of fields. If X and Y are two transcendence bases for L over K, then either both X and Y are finite and $|X| = |Y|$ or both X and Y are infinite.*

This justifies the following definition.

Definition 2.7. The *transcendence degree* of a field extension L over K is the cardinality of any transcendence basis for the extension.

We will need to understand algebra-finite field extensions. Below we show that for field extensions algebra finite is equivalent to module-finite which is equivalent to finite (degree) extension.

Lemma 2.8 (Zariski's Lemma)**.** *Let $K \subseteq L$ be fields. If L is a finitely generated K-algebra, then L is a finite dimensional K-vector space. In particular, if K is algebraically closed then $L = K$.*

Proof. Let $L = K[h_1, \ldots, h_d]$. Since in particular $h_1, \ldots, h_d$ generate L as a field over K, we can choose a transcendence basis for L/K from among the h's, and after reordering, we may assume that $h_1, \ldots, h_c$ form a transcendence basis, and $h_{c+1}, \ldots, h_d$ are algebraic over $K' = K(h_1, \ldots, h_c) = \mathrm{Frac}(K[h_1, \ldots, h_c])$. Since $h_1, \ldots, h_c$ form a transcendence basis, these elements are algebraically independent and so $K[h_1, \ldots, h_c]$ is a free K-algebra.

Then L is integral and algebra-finite over K', hence module-finite. Thus, if $c = 0$, we are done. Suppose that $c \neq 0$; we will obtain a contradiction to complete the proof.

We can apply the Artin-Tate Lemma to $K \subseteq K' \subseteq L$ to see that K' is algebra-finite over K. In particular, there are f_i, g_i in the polynomial ring $K[h_1, \ldots, h_c]$ such that $K' = K[\frac{f_1}{g_1}, \ldots, \frac{f_c}{g_c}]$. This implies that any element of K' can be written as a fraction with denominator $(g_1 \cdots g_c)^n$ for some n. The element $\frac{1}{g_1 \cdots g_c + 1} \in K'$ cannot be written this way; if so, we would have

$$\frac{v}{(g_1 \cdots g_c)^n} = \frac{1}{g_1 \cdots g_c + 1},$$

for some $v \in K[h_1, \ldots, h_c]$ with $g_1 \cdots g_c \nmid v$ (since the polynomial ring $K[h_1, \ldots, h_c]$ is a UFD). But, the equation $g_1 \cdots g_c v + v = (g_1 \cdots g_c)^n$ contradicts this.

Now if K is algebraically closed and $\ell \in L$, since L/K is finite then ℓ is algebraic over K, thus $\ell \in K$. □

Example 2.9. Let K be a field and $\mathfrak{m}$ a maximal ideal of the polynomial ring $K[x_1, \ldots, x_n]$ for some n. Then $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finitely generated K algebra and hence by Zariski's Lemma 2.8 $K \hookrightarrow K[x_1, \ldots, x_n]/\mathfrak{m}$ is finite field extension (or, more precisely, $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finte extenion of the image of K under the quotient map $K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/\mathfrak{m}$).

For example if $K = \mathbb{R}$, then for every maximal ideal $\mathfrak{m}$ of $\mathbb{R}[x_1, \ldots, x_n]$ we have that $\mathbb{R}[x_1, \ldots, x_n]/\mathfrak{m}$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. Both do occur; for example $\mathbb{R}[x](x - r) \cong \mathbb{R}$ for any $r \in \mathbb{R}$ and $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

If K is algebraically closed, for example if $K = \mathbb{C}$, then the map $K \hookrightarrow K[x_1, \ldots, x_n]/\mathfrak{m}$ must be an isomorphism for every maximal ideal $\mathfrak{m}$.

Now we can prove Theorem 2.3.

Proof of Theorem 2.3. To see that the map is well defined observe that the ideal $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$ of $K[x_1, \ldots, x_n]$ is maximal, since

$$K[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \xrightarrow{\cong} K.$$

by means of the evaluation map

$$x_1 \mapsto a_1, \ldots, x_n \mapsto a_n.$$

Now for the surjectivity of the map

$$\mathbb{A}^n_K \to \{\text{maximal ideals of } K[x_1, \ldots, x_n]\}.$$

Suppose $\mathfrak{m}$ is a maximal ideal of $K[x_1, \ldots, x_n]$. Then, since $K \hookrightarrow K[x_1, \ldots, x_n]/\mathfrak{m}$ is algebra-finite then $K \hookrightarrow K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension by Lemma 2.8 and furthermore since $K = \overline{K}$ there must be an isomorphism:

$$K \xrightarrow{\cong} K[x_1, \ldots, x_n]/\mathfrak{m}.$$

Let $a_1, \ldots, a_n \in K$ be the preimages of $x_1 + \mathfrak{m}, \ldots, x_n + \mathfrak{m}$ under this isomorphism. Then $x_i - a_i + \mathfrak{m} = 0$ for all i and hence

$$(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}.$$

But these are both maximal ideals and so they must in fact be equal.

Lastly the map is one to one because if $(x_1 - a_1, \ldots, x_n - a_n) = (x_1 - a'_1, \ldots, x_n - a'_n) = \mathfrak{m}$, then $a'_i - a_i = (x_i - a_i) - (x_i - a'_i) \in \mathfrak{m}$ for all i. Since $a'_i - a_i$ belongs to K, if it was not 0 it would be a unit, but then it would not belong to the proper ideal $\mathfrak{m}$. So we must have $a_i = a'_i$ for all i. □

February 15, 2021

2.1.2 The ideal-algebraic set correspondence

Starting with a system of equations we can consider its set of solutions .

Definition 2.10. For a subset T of the ring $K[x_1, \ldots, x_n]$, we define the subset $V(T)$ of $\mathbb{A}^n_K$ to be the set of common zeros or the *zero set* or *vanishing set* of the members (equations) in T:

$$V(T) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in T\}.$$

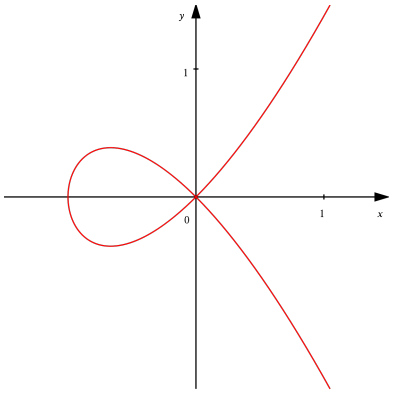
Sometimes, in order to emphasize the role of K, we will write this as $V_K(T)$.

Definition 2.11. A subset of $\mathbb{A}_k^n$ of the form $V(T)$ for some subset $T \subseteq K[x_1, \ldots, x_n]$ is called an *algebraic subset* of $\mathbb{A}_k^n$. In other words, an algebraic subset of $\mathbb{A}_k^n$ is the set of simultaneous solutions of some (possibly infinite) collection of polynomial equations.

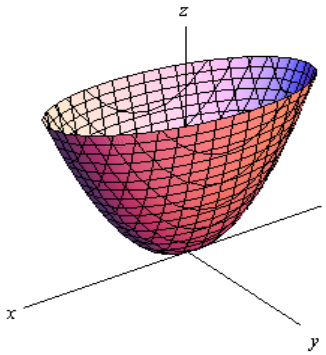
Definition 2.12. An irreducible algebraic set, i.e. an algebraic set that cannot be written as the union of two proper algebraic subsets, is called an *affine algebraic variety*.

Example 2.13. Here are some simple examples of algebraic sets:

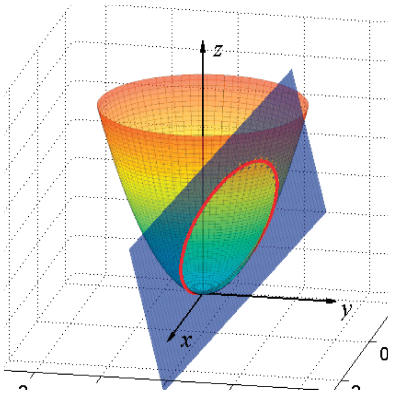
- For $K = \mathbb{R}$ and $n = 2$, $V(y^2 + x^2(x+1))$ is a "nodal curve" in $\mathbb{A}^2_{\mathbb{R}}$, the real plane. Note that we've written x for x_1 and y for x_2 here.



- For $K = \mathbb{R}$ and $n = 3$, $V(z - x^2 - y^2)$ is a paraboloid in $\mathbb{A}^3_{\mathbb{R}}$, real three space. Note that $x = x_1$, $y = x_2$ and $z = x_3$.



- For $K = \mathbb{R}$ and $n = 3$, $V(z - x^2 - y^2, 3x - 2y + 7z - 7)$ is circle in $\mathbb{A}^3_{\mathbb{R}}$.



- **The field matters:** $V_{\mathbb{R}}(x^2+y^2+1) = \emptyset$, while $V_{\mathbb{C}}(x^2+y^2+1) \neq \emptyset$.
- For any field K and elements $a_1, \ldots, a_n \in K$, we have

$$V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

  So, all one element subsets of $\mathbb{A}^n_K$ are algebraic subsets.

- Different systems of polynomial equations can have the same solutions: the origin in $\mathbb{A}^n_K$ is given by

$$V(x_1, \ldots, x_n) = V(x_1^2, \ldots, x_n^2) = \{(0, 0, \ldots, 0)\}.$$

Example 2.14. Here are some examples of sets that are **not algebraic**:

- The set $X = \{(x, y) \in \mathbb{A}^2_{\mathbb{R}} \mid y \geq 0\}$.

  Suppose $f(x, y) = 0$ for every $(x, y) \in X$. Viewing $f \in \mathbb{R}[x, y] = \mathbb{R}[x][y]$ we can write

$$f(x, y) = y \cdot g(x, y) + h(x)$$

  for some polynomials $g \in \mathbb{R}[x, y], h \in \mathbb{R}[x]$. Since $(x, 0) \in X$, we have $f(x, 0) = 0$ for each $x \in \mathbb{R}$. Thus $h(x) = 0$ for all $x \in \mathbb{R}$ and thus $h(x) = 0$. It follows that y divides f.

  Similarly, for each $a \in \mathbb{R}$ we can write

$$f(x, y) = (y - a) \cdot g(x, y) + h(x).$$

  If $a \geq 0$, we have $(x, a) \in X$ for all $x \in \mathbb{R}$, so $f(x, a) = 0$ and this yields $(y-a) \mid f$ by the same argument as above.

  In the UFD $\mathbb{R}[x, y]$ we now have that f is divisible by infinitely many non-associate irreducible polynomials $y - a$ with $a \geq 0$. This is only possible if $f = 0$.

  We have established that if $X = V(T)$ then $T = \{0\}$. But $V(0) = \mathbb{A}^2_{\mathbb{R}}$, a contradiction.

- The subset $A_K^2 \setminus \{(0,0)\}$ is not an algebraic subset of $\mathbb{A}_K^2$ if K is infinite. Why?
- The graph of the sine function is not an algebraic subset of $\mathbb{A}_{\mathbb{R}}^2$. Why not?

We can also go the opposite way: start with a subset of affine space and consider the equations that it satisfies.

Definition 2.15. Given any subset X of $\mathbb{A}_K^n$ for a field K, define

$$I(X) = \{g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \mid g(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in X\}$$

Lemma 2.16. *For any subset X of $\mathbb{A}_K^n$, $I(X)$ is an ideal of $K[x_1, \ldots, x_n]$.*

Proof. Clear from the definition. □

Example 2.17.
- $I(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n)$, for any field k.
- $I(\{(x, y) \in \mathbb{A}_{\mathbb{R}}^2 \mid y \geq 0\}) = (0)$.

Proposition 2.18 (Properties)**.** *Here are some properties of the functions V and I:*

1. *For any field, we have $V(0) = \mathbb{A}_K^n$ and $V(1) = \emptyset$.*
2. *If $I \subseteq J \subseteq K[x_1, \ldots, x_n]$ then $V(I) \supseteq V(J)$.*
3. *If $I, J \subseteq K[x_1, \ldots, x_n]$ then*
$$V(I + J) = V(I) \cap V(J) \text{ and } V(I \cap J) = V(I) \cup V(J).$$
4. *$I(\emptyset) = (1) = K[x_1, \ldots, x_n]$ (the improper ideal).*
5. *$I(\mathbb{A}_K^n) = (0)$ if and only if K is infinite.*
6. *If $S \subseteq T$ are subsets of $\mathbb{A}_K^n$ then $I(S) \supseteq I(T)$.*

In regards to the fifth property, notice that if $K = \{k_1, \ldots, k_s\}$ is a finite field, then the following polynomial is a non zero element of $I(\mathbb{A}_K^n)$:

$$f = \prod_{i=1}^{n} \prod_{j=1}^{s} (x_i - k_j)$$

Exercise 2.19. Supply a proof to the previous Proposition.

February 17, 2021

Definition 2.20. For any ideal I in an arbitrary ring R the *radical* of I, is

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

We say an ideal I is *radical* if $I = \sqrt{I}$.

Example 2.21. The ideal (x^2) of $K[x]$ has radical $\sqrt{(x^2)} = (x)$, so it is not a radical ideal. However (x) is a radical ideal since $\sqrt{(x)} = (x)$.

The above example is a bit misleading. In general, to compute the radical of an ideal it is not enough to take "radicals" of the generators by removing powers higher than 1. This approach does work however for ideals generated by monomials.

Proposition 2.22 (Properties of radicals)**.** *1. for any ideal I we have $I \subseteq \sqrt{I}$*

2. for any ideal I we have that $\sqrt{I}$ is a radical ideal, i.e. $\sqrt{\sqrt{I}} = \sqrt{I}$.

3. all prime ideals and in particular all maximal ideals are radical.

4. the improper ideal R is radical.

The image of the function I lands in the set of radical ideals:

Lemma 2.23. *If X is a subset of $\mathbb{A}^n_K$ then $I(X)$ is a radical ideal.*

Proof. We show that $\sqrt{I(X)} = I(X)$: let $f \in \sqrt{I(X)}$, then $f^N \in I(X)$ for some $N \in \mathbb{N}$ and thus

$$f(a_1, \ldots, a_n)^N = 0 \text{ in } K \text{ for each } (a_1, \ldots, a_n) \in X.$$

It follows that $f(a_1, \ldots, a_n) = 0$ for each $(a_1, \ldots, a_n) \in X$, i.e. $f \in I(X)$. □

We nexts show that we can adjust the source of the function V to be the set of radical ideals without reducing its image.

Proposition 2.24. *For a subset T of $K[x_1, \ldots, x_n]$ we have*

$$V(T) = V((T)) = V(\sqrt{(T)})$$

where (T) denotes the ideal generated by T.

Proof. Each of $\supseteq$ is clear from the properties of V and the containments

$$T \subseteq (T) \subseteq \sqrt{(T)}$$

Suppose $a := (a_1, \ldots, a_n) \in V(T)$. Then a is a root of each $f \in T$ and hence it is a root of anything of the form $\sum_i g_i f_i$ with $g_i \in k[x_1, \ldots, x_n]$. That is, $a \in V((T))$. For any $f \in \sqrt{(T)}$, we have $f^n \in (T)$ for some n and hence $f^n(a) = (f(a))^n = 0$, whence $f(a) = 0$ (since K is a reduced ring). □

Corollary 2.25. *Every algebraic set can be written as $V(I)$ for a radical ideal I.*

Proof. If $X \subseteq \mathbb{A}^n_K$ is an algebraic set then $X = V(T)$ for some subset $T \subseteq K[x_1, \ldots, x_n]$. Now take $I = \sqrt{(T)}$, which is a radical ideal by the properties of radicals and satisfies $X = V(I)$ by the previous proposition. □

Corollary 2.26. *Every algebraic subset of $\mathbb{A}_k^n$ is the set of simultaneous solutions of some finite set of polynomial equations.*

Proof. By Proposition 2.24, every algebraic subset as has the form $V(I)$ for some ideal (in fact, for some radical ideal) I. By the Hilbert basis theorem, $I = (f_1, \ldots, f_m)$ for some $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ and hence $V(I) = V(\{f_1, \ldots, f_m\})$. □

Henceforth we will thus restrict ourselves to considering the correspondences

$$\{\text{radical ideals in } K[x_1, \ldots, x_n]\} \underset{V}{\overset{I}{\leftrightarrows}} \{\text{algebraic subsets of } \mathbb{A}_K^n\}$$

We finally answer our Question 2.1 by the following correspondence, which says that an algebraic set uniquely determines its largest system of equations, which is a radical ideal.

Theorem 2.27 (Ideal-algebraic set correspondence)**.** *When K is an algebraically closed field, the functions*

$$I : \{ \textit{ algebraic subsets of } \mathbb{A}_k^n \} \to \{ \textit{ radical ideals of } k[x_1, \ldots, x_n] \}$$

and

$$V : \{\textit{radical ideals of } k[x_1, \ldots, x_n]\} \to \{ \textit{ algebraic subsets of } \mathbb{A}_k^n \}$$

are mutually inverse, order-reversing bijections of posets.

We first prove an important particular case in which $V(J) = \emptyset$ determines J.

Theorem 2.28 (Hilbert's Nullstellensatz (Weak Form))**.** *Let K be an algebraically closed field, and suppose J is an ideal of $K[x_1, \ldots x_n]$. We have*

$$V(J) = \emptyset \textit{ if and only if } J = K[x_1, \ldots, x_n].$$

Remark 2.29. One direction is easy. The non-trivial direction, in it's most basic form, says the following: Suppose we are given a system of polynomial equations

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ \vdots &= \vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

in n variables with coefficients in some algebraically closed field K. If the system has no solutions over K, then for some polynomials $g_1, \ldots, g_m$ we have $\sum_i g_i f_i = 1$. (The converse is clear.)

For example, when $n = 1$, it says that if $f_1(x), \ldots, f_m(x)$ do not share a common root in K, then their collective gcd is 1. This case is easy to prove, and is essentially equivalent to the definition of "algebraically closed". It's much harder and much less obvious for $n > 1$.

Proof. If $J = K[x_1, \ldots, x_n]$, then $V(J) = \emptyset$ since $1 = 0$ has no solutions.

We show that if $J \subset K[x_1, \ldots, x_n]$ is a proper ideal, then $V(J) \neq \emptyset$. Since J is proper, it is contained in some maximal ideal $\mathfrak{m}$. Since K is algebraically closed, by Theorem 2.3 we know $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_i \in K$. Since $J \subseteq (x_1 - a_1, \ldots, x_n - a_n)$, we have

$$V(J) \supseteq V((x_1 - a_1, \ldots, x_n - a_n)) = \{a_1, \ldots, a_n\}.$$

□

February 19, 2021

To attack the Strong Form of the Nullstellensatz, we will need an observation on inequations.

Remark 2.30 (Rabinowitz's trick). We write $\underline{x} = (x_1, \ldots, x_n)$ and $\underline{a} = (a_1, \ldots, a_n)$. Observe that, if $f(\underline{x})$ is a polynomial, $f(\underline{a}) \neq 0$ if and only if there is a solution $y = b \in K$ to $yf(\underline{a}) - 1 = 0$. In particular, a system of polynomial equations and inequations

$$f_1(\underline{x}) = 0, \ldots, f_m(\underline{x}) = 0, g_1(\underline{x}) \neq 0, \ldots, g_n(\underline{x}) \neq 0$$

has a solution $\underline{x} = \underline{a}$ if and only if the system

$$f_1(\underline{x}) = 0, \ldots, f_m(\underline{x}) = 0, y_1 g_1(\underline{x}) - 1 = 0, \ldots, y_n g_n(\underline{x}) - 1 = 0$$

has a solution $(\underline{x}, \underline{y}) = (\underline{a}, \underline{b})$. In fact, this is equivalent to a system in one extra variable:

$$f_1(\underline{x}) = 0, \ldots, f_m(\underline{x}) = 0, y g_1(\underline{x}) \cdots g_n(\underline{x}) - 1 = 0.$$

Theorem 2.31 (Hilbert's Nullstellensatz (Strong Form))**.** *Let K be a an algebraically closed field and let J be an ideal in the polynomial ring $R = K[x_1, \ldots, x_n]$. Then*

$$I(V(J)) = \sqrt{J}.$$

Remark 2.32. The Strong Form implies the Weak Form: If $V(J)$ is empty, then $1 \in I(V(J))$ and hence $1^n \in J$ by the Strong Form, which gives that $J = (1)$.

Proof. By Proposition 2.24 the equations in $\sqrt{J}$ vanish on $V(J)$, so $\sqrt{J} \subseteq I(V(J))$.

For the converse, suppose that $f(\underline{x})$ vanishes on $V(J)$. Let $J = (g_1, \ldots, g_m)$. Considering the system

$$g_1(\underline{x}) = 0, \ldots, g_m(\underline{x}) = 0, f(\underline{x}) \neq 0.$$

If $\underline{a}$ is a solution for the first m equations then $\underline{a} \in V(g_1, \ldots, g_m) = V(J)$. Since f vanishes on $V(J)$ we see that $f(\underline{a}) = 0$, which contradicts the last equation. Hence the system above has no solution. By the remark above, this implies that

$$Z(JS + (yf - 1)) = \varnothing,$$

where $JS + (yf - 1)$ is an ideal in the polynomial ring $R = K[x_1, \ldots, x_n, y]$. By the Weak Nullstellensatz, we see that $1 \in JS + (yf - 1)$. Write $J = (g_1(\underline{x}), \ldots, g_m(\underline{x}))$, and

$$1 = r_0(\underline{x}, y)(1 - yf(\underline{x})) + r_1(\underline{x}, y)g_1(\underline{x}) + \cdots + r_m(\underline{x}, y)g_m(\underline{x}).$$

We can apply an evaluation map $R \to \mathrm{Frac}(R)$ sending $y \mapsto 1/f$ to get

$$1 = r_1(\underline{x}, 1/f)g_1(\underline{x}) + \cdots + r_m(\underline{x}, 1/f)g_m(\underline{x}).$$

Since each r_i is polynomial, there is a largest negative power of f occurring; say that f^n serves as a common denominator. We can clear denominators multiplying by f^n to obtain (on the LHS) f^n as a polynomial combination of the g's (on the RHS). Thus $f \in J$. □

Proof of Theorem 2.27. The Nullstellensatz gives $I(V(J)) = J$ for any radical ideal J.

Given an algebraic set X we have by definition and Corollary 2.25 that $X = V(J)$ for some radical ideal J. So $V(I(X)) = V(I(V(J)) = V(J) = X$ by the Nullstellensatz again. □

Remark 2.33. In fact, $V(I(X)) = X$ holds for any field and any algebraic subset X: If $\underline{a} \in X$, then for any $g \in I(X)$, $g(\underline{a}) = 0$ by definition and thus $\underline{a} \in V(I(X))$. Conversely, we use that $X = V(J)$ for some ideal J, and so if $\underline{a} \notin X$, then $g(\underline{a}) \neq 0$ for some $g \in J$. But $g \in I(X)$ by the definitions, and so $\underline{a} \notin V(I(X))$.

Thus, in the statement of the Corollary, $V \circ I$ is the identity, and so I is an injection and V is a surjection for any field K. But I will fail to be onto and Z can fail to be injective, for a non-algebraically closed field K.

2.2 The category of algebraic sets and algebraic morphisms

We now make the collection of algebraic subsets into a category. For simplicity, we'll restrict attention to algebraically closed fields, although much of this holds for any field.

Definition 2.34. Suppose X is an algebraic subset of $\mathbb{A}^n_K$ and Y is an algebraic subset of $\mathbb{A}^m_K$. A *morphism of algebraic sets* or *algebraic map* or *regular map* from X to Y is a set-theoretic function $G : X \to Y$ defined coordinatewise by polynomials $g_1, \cdots, g_m \in K[x_1, \ldots, x_n]$, that is

$$G(a_1, \ldots, a_n) = (g_1(a_1, \ldots, a_n), \cdots, g_m(a_1, \ldots, a_n)) \text{ for all } \underline{a} \in X.$$

Not every choice of $g_1, \cdots, g_m$ will give such a morphism, because the tuple $(g_1(\underline{a}), \cdots, g_m(\underline{a}))$ has to satisfy the equations of Y.

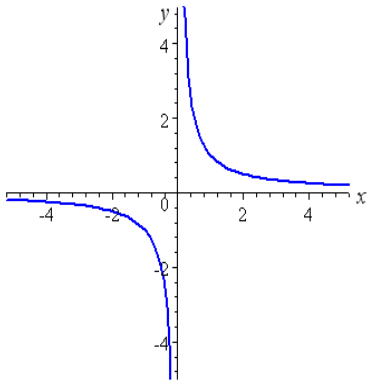
Example 2.35. For each algebraic variety X we get an identity morphism by setting $g_i(x_1, \ldots, x_n) = x_i$ in the definition above

$$\mathrm{id}_X : X \to X, \mathrm{id}_X(a_1, \ldots, a_n) = (a_1, \ldots, a_n) \text{ for all } \underline{a} \in X.$$

Definition 2.36. Two algebraic subsets X and Y are isomorphic if there are algebraic maps $G : X \to Y$ and $H : Y \to X$ such that $G \circ H = \mathrm{id}_Y$ and $H \circ G = \mathrm{id}_X$, in which case each of G an H is referred to as an *isomorphism* of algebraic sets.

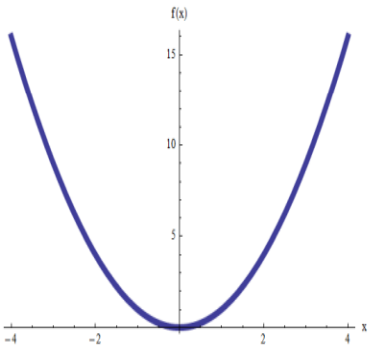
Remark 2.37. An isomorphism of algebraic sets must be a bijection, but the converse is not true (see the second example below).

Example 2.38. Let $X = V(xy - 1) \subseteq \mathbb{A}^2_K$ (i.e., X is a hyperbola) and define $G : X \to \mathbb{A}^1_K$ by $G(a, b) = a$. Then G is an algebraic map (indeed, it's given by a linear polynomial) and its image is $\mathbb{A}^1_K \setminus \{0\}$, which is *not* an algebraic subset of $\mathbb{A}^1_K$. So, **the set-theoretic image of a morphism of algebraic sets need not be algebraic**.



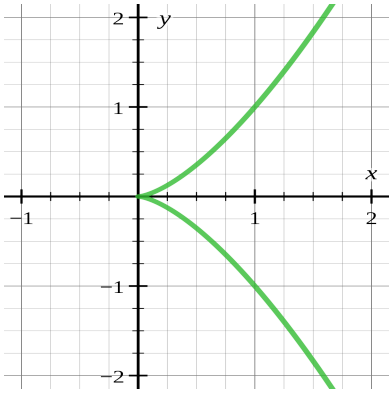
February 22, 2021

Example 2.39. Let $Z = V(y - x^2)$ be the parabola (graph of $f(x) = x^2$). Then Z is isomorphic to $\mathbb{A}^1_K$ via the mutually inverse morphisms $G : Z \to \mathbb{A}^1_K, G(x, y) = x$ and $H : \mathbb{A}^1_K \to Z, H(x) = (x, x^2)$.



Example 2.40. Let Y be the classical cuspidal curve:

$$Y = Z(y^2 - x^3) \subseteq \mathbb{A}^2_K.$$



Define

$$G : \mathbb{A}^1_K \to Y \quad G(t) = (t^2, t^3).$$

G is an algebraic map from $\mathbb{A}^1_K$ to Y since the component functions are polynomial functions of t and $(t^3)^2 - (t^2)^3 = 0$ for all t.

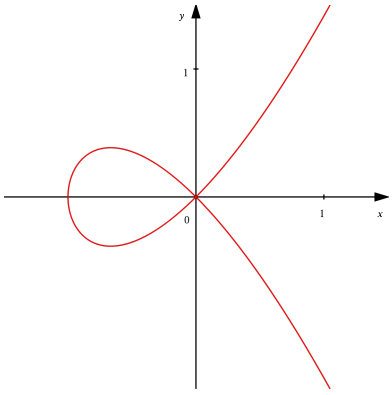
Note that G **is a bijection of sets, but, it is *not* an isomorphism of algebraic subsets**! There does not exist an algebraic morphism

$$H : Y \to \mathbb{A}^1_K$$

such that $G \circ H$ and $H \circ G$ are both the identity function. We will justify this later.

Example 2.41. Let X be the classical nodal curve in $\mathbb{A}^2_K$ given by

$$X = V(y^2 - x^2(x + 1)).$$



Define an algebraic map

$$G : \mathbb{A}^1_K \to X \quad G(t) = (t^2 - 1, t^3 - t).$$

G is an algebraic morphism since it is represented by polynomials functions and for any $t \in \mathbb{A}^1_K$, we have $G(t) \in X$ since

$$(t^3 - t)^2 - (t^2 - 1)^2(t^2 - 1 + 1) = t^6 - 2t^4 + t^2 - (t^4 - 2t^2 + 1)t^2 = 0.$$

The function G is surjective and the preimage of every point on X is single point with one exception: the fiber of $(0, 0) \in Z$ consists of two points, 1 and -1, provided $\mathrm{char}(K) \neq 2$. Since G is not a set-theoretic bijection it cannot be an isomorphism.

Theorem 2.42. *The collections of affine algebraic sets over a fixed field K and the algebraic maps between them form a category $\langle\langle$Algebraic Sets$\rangle\rangle_K$.*

A few remarks on this, instead of an honest proof:

- the objects of this category are really pairs (X, n) where X is an algebraic subset of $\mathbb{A}^n_K$. However, we will usually refer to objects as just X.
- the morphisms between $X \subseteq \mathbb{A}^n_K$ and $Y \subseteq \mathbb{A}^m_K$ are

  $$\mathrm{Hom}_{\langle\langle \text{Algebraic-Sets}\rangle\rangle_K}(X, Y) = \{G : X \to Y \mid G(\underline{x}) = (g_1(\underline{x}), \ldots, g_m(\underline{x})), g_i \in K[x_1, \ldots, x_m]\}$$

- I will not prove this carefully, but note that the composition of two morphisms of algebraic sets $F : X \to Y$, $G : Y \to Z$ is their composition as functions. This is a morphism of algebraic sets, as the composition of two polynomial maps is a polynomial.
- as seen in Example 2.35 each algebraic set X is equipped with an identity morphisms id_X

Remark 2.43. It is important to note that the morphisms described above and in Definition 2.34 are viewed as functions. In particular different tuples of polynomials $g_1, \ldots, g_m$ can determine the same morphism G.

Lemma 2.44. *Let X be an algebraic subset of $\mathbb{A}^n_K$ and let $f, g \in \mathrm{Hom}_{\langle\langle \text{Algebraic-Sets}\rangle\rangle_K}(X, \mathbb{A}^1_K)$. Then $f = g$ if and only if there is an equality of equivalence classes $\overline{f} = \overline{g}$ in*

$$\frac{K[x_1, \ldots, x_n]}{I(X)}.$$

Proof. We have

$$\begin{aligned} f = g \text{ in } \mathrm{Hom}_{\langle\langle \text{Algebraic-Sets}\rangle\rangle_K}(X, \mathbb{A}^1_K) &\iff f(\underline{a}) = g(\underline{a}) \text{ for all } \underline{a} \in X \\ &\iff (f - g)(\underline{a}) = 0 \text{ for all } \underline{a} \in X \\ &\iff f - g \in I(X) \\ &\iff \overline{f} = \overline{g} \text{ in } \frac{K[x_1, \ldots, x_n]}{I(X)} \end{aligned}$$

□

We fix this issue by considering a better ring of functions.

Definition 2.45. For an algebraic subset X of $\mathbb{A}^n_K$, the *coordinate (function) ring* or the *ring of regular functions* of X is the K-algebra

$$K[X] := K[x_1, \ldots, x_n]/I(X).$$

Definition 2.46. We call an *affine K-algebra* any ring of the form

$$K[x_1, \ldots, x_n]/I_A \text{ for some ideal } I_A \subseteq K[x_1, \ldots, x_n].$$

Definition 2.47. An algebra A is *reduced* if $a^n = 0$ implies $a = 0$ in A.

We now see that coordinate rings have both of these properties.

Lemma 2.48. *If X is an algebraic set then $K[X]$ is a reduced affine K-algebra.*

Conversely, if K is an algebraically closed field then any reduced affine K-algebra is a coordinate ring.

Proof. Recall that $I(X)$ is a radical ideal. Then for $f \in K[x_1, \ldots, x_n]$, $\overline{f}^n = 0$ in $K[X]$ if and only if $f^n \in I(X)$ if and only if $f \in \sqrt{I(X)} = I(X)$ if and only if $\overline{f} = 0$ in $K[X]$.

Conversely, let $A = K[x_1, \ldots, x_n]/J$ be an affine K-algebra. Then A is reduced if and only if $J = \sqrt{J}$. Setting $X = V(J)$ and using the strong Nullstellensatz gives $I(X) = I(V(J)) = \sqrt{J} = J$. Thus $A = K[X]$. □

Remark 2.49. The generators of the coordinate ring $K[X]$ as a K-algebra are the *coordinate functions* a.k.a. the projection functions onto each of the n coordinates: $x_i : X \to \mathbb{A}^K_1, x_i(\underline{a}) = a_i$.

February 24, 2021

We now enhance Lemma 2.48 to another important correspondence in algebraic geometry: algebraic sets are uniquely determined by their coordinate rings.

In the following we consider the category of algebraic sets over a fixed field K defined previously and the category of reduced affine K-algebras. The morphisms in the latter category are K-algebra morphisms. In other words, this is a full subcategory of $\langle\langle$K-Algebras$\rangle\rangle$.

Theorem 2.50 (Algebraic set–coordinate ring correspondence)**.** *For an algebraically closed field K, the following categories are equivalent*

$$\langle\langle \textit{Algebraic Sets} \rangle\rangle_K \cong \langle\langle \textit{Reduced affine } K\textit{-algebras} \rangle\rangle$$

Proof sketch. An equivalence may be given by the contravariant functors

$$\Phi : \langle\langle \text{Algebraic Sets} \rangle\rangle \to \langle\langle \text{Reduced affine } K\text{-algebras} \rangle\rangle$$

$$X \mapsto K[X] \text{ and } (G : X \to Y) \mapsto \Phi(G)$$

where $\Phi(G)$ is defined as follows: For each algebraic set morphism

$$G : X \to Y, G = (g_1, \ldots, g_m), g_i \in K[x_1, \ldots, x_n],$$

let $\Phi(G) : K[Y] \to K[X]$ be given by

$$\Phi(G)(f(y_1, \ldots, y_m)) = f(g_1(\underline{x}), \ldots, g_m(\underline{x})) = (f \circ G).$$

An inverse of Φ may be given by the functor

$$\Psi : \langle\langle \text{Affine } K\text{-algebras} \rangle\rangle \to \langle\langle \text{Algebraic Sets} \rangle\rangle$$

defined on objects as follows:

$$K[x_1, \ldots, x_n]/J \mapsto V(J).$$

Let $g : A \to B$ be a morphism of affine K-algebras. Set $A = K[x_1, \ldots, x_m]/I_A$ and $B = K[x_1, \ldots, x_n]/I_B$ and let $\overline{f}_i := g(\overline{x_i}) \in B$ and let $f_i \in K[x_1, \ldots, x_n]$ be any representative for the coset $\overline{f_i}$. The functor Ψ sends g to the morphism of algebraic varieties $\Psi(g) : V(I_B) \to V(I_A)$ given by

$$\Psi(g) : V(I_B) \to V(I_A), \quad \Psi(g)(b_1, \ldots, b_n) = (f_1(b_1, \ldots, b_n), \ldots, f_m(b_1, \ldots, b_n)).$$

Let's check that the image of the map above really lands in $V(I_A)$. Indeed, if $f \in I_A$ then $\overline{f} = 0$ in A and so $g(f) \in I_B$. Using this,

$$f(\Psi(g)(b_1, \ldots, b_n)) = f(f_1(b_1, \ldots, b_n), \ldots, f_m(b_1, \ldots, b_n)) = g(f(b_1, \ldots, b_n)) = 0,$$

which shows that $\Psi(g)(I_B) \subseteq V(I_A)$. □

The following is an immediate consequence of the theorem.

Corollary 2.51. *For any field K, a pair of algebraic subsets X and Y are isomorphic if and only if their coordinate function rings $K[X]$ and $K[Y]$ are isomorphic K-algebras.*

Proof. If G and H are mutually inverse morphisms of algebraic varieties X and Y then $\Phi(G)$ and $\Phi(H)$ are mutually inverse morphisms of their coordinate rings $K[X]$ and $K[Y]$ by properties of functors.

Similarly, if f and g are mutually inverse morphisms of coordinate rings $K[X]$ and $K[Y]$ then $\Psi(f)$ and $\Psi(g)$ are mutually inverse morphisms of algebraic varieties X, Y. □

Let's illustrate the use of this corollary with some examples:

Example 2.52 (Compare with Example 2.40)**.** Assume K is an algebraically closed field. The cuspidal cubic $X = Z(y^2 - x^3)$ is not isomorphic to $\mathbb{A}^1_K$, even though there is a bijective algebraic morphism $G : \mathbb{A}^1_K \to X$ given by $a \mapsto (a^3, a^3)$.

Let's consider $\Phi(G) : K[X] = K[x,y]/(y^2 - x^3) \to K[\mathbb{A}^1_K] = K[t]$, that is the K-algebra homomorphism given by $x \mapsto t^2, y \mapsto t^3$. The image of this map is $K[t^2, t^3]$ and in fact

$$K[X] = K[x,y]/(y^2 - x^3) \cong K[t^2, t^3] \subsetneq K[t].$$

Since $\Phi(G)$ is not surjective we see that G cannot be an isomorphism of algebraic sets.

To see that there is *no* isomorphism of algebraic sets between X and $\mathbb{A}^1_K$ note that if there were such an isomorphism, then we would have an isomorphism of K-algebras $K[t] \cong K[x,y]/(y^2 - x^3)$. But this is impossible since $K[x,y]/(y^2 - x^3)$ isn't a PID: the ideal (x,y) isn't principal.

Let's prove $k[x,y]/(y^2 - x^3)$ isn't a PID: If it were, then the image J of I in the quotient ring $R/(x^2, xy, y^2) = k[x,y]/(x^2, xy, y^2)$ of R would also be principal. That is we would have $(x,y) = (g)$ in $k[x,y]/(x^2, xy, y^2)$ for some $g = ax + by +$ higher order terms. As a k-vector space (x,y) is two dimensional and any such g would generate an ideal that is merely (at most) one-dimenisonal, and hence this is not possible.

Example 2.53 (Compare with Example 2.39)**.** The parabola $V(y - x^2)$ is isomorphic to $\mathbb{A}^1_K$, for any algebraically closed field K. This is true since

$$K[x,y]/(y - x^2) \cong K[x]$$

as K-algebras.

A similar result holds for the graph of any polynomial $f(x)$.

Example 2.54. One must be a little careful for non-algebraically closed fields. Note that for $K = \mathbb{R}$, the algebraic subsets $V(x^2 + y^2 + 1)$ and $\emptyset$ are isomorphic, but the K-algebras $K[x,y]/(x^2 + y^2 + 1)$ and $K[x,y]/(1) = 0$ are not. This doesn't contradict the Theorem since $(x^2 + y^2 + 1)$ is not equal to $I(X)$ for any X.

2.3 The prime spectrum and the Zariski topology

We have thus far associated to each algebraic X set a ring, $K[X]$, its coordinate ring, which you should think of as the ring of functions $X \to K = \mathbb{A}^1_K$. We now go the opposite way: given $K[X]$ how do we recover the underlying set X? We can recover the points of X as the set of maximal ideals of $K[X]$ since the maximal ideals of $K[X]$ are in correspondence with the points of X. We have technically only proven this for $X = \mathbb{A}^n$ in Theorem 2.3 but this implies the general case.

More generally, for an arbitrary ring R, not necessarily an affine algebra, if we think of R as functions on a mystery space Z what should Z look like? A first attempt at an answer would be the set of maximal ideals of R. However this answer is not satisfying as it is not functorial: given a ring map $R \to S$, the maximal ideals of S do

not necessarily correspond to maximal ideals of R. To fix this we must enlarge the set of ideals we consider to all prime ideals. So the correct answer is $Z = \mathrm{Spec}(R)$ and we can make this into a topological space.

Definition 2.55.

- The *prime spectrum* or *spectrum* of a ring R is the set

$$\mathrm{Spec}(R) = \{\mathfrak{p} \mid \mathfrak{p} \text{ a prime ideal of } R\}.$$

- The *maximal spectrum* of a ring R is the set

$$\mathrm{mSpec}(R) = \{\mathfrak{m} \mid \mathfrak{m} \text{ a maximal ideal of } R\}.$$

Definition 2.56. A *topological space* is a set X together with a collection of subsets of X called the closed sets. They must satisfy:

1. The empty set and X itself are closed.
2. A finite union of closed sets is closed.
3. An arbitrary intersection of closed sets is closed.

Definition 2.57. Let R be a ring. The *Zariski topology* on $\mathrm{Spec}(R)$ is defined by taking the *Zariski closed sets* to be the sets $\mathbb{V}(I)$ for all (proper and improper) ideals $I \subseteq R$, where

$$\mathbb{V}(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}$$

February 24, 2021

Proposition 2.58 (Properties of Zariski closed sets)**.** *For any ideals $I, J, I_1, \ldots, I_n$ of a ring R we have*

1. $\mathbb{V}(R) = \emptyset$
2. $\mathbb{V}((0)) = \mathrm{Spec}(R)$
3. $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup V(J)$ *and more generally* $\mathbb{V}(I_1 \cap \cdots \cap I_n) = \mathbb{V}(I_1) \cup \cdots \cup V(I_n)$
4. $\mathbb{V}(I + J) = \mathbb{V}(I) \cap V(J)$ *and more generally* $\mathbb{V}(\sum_{I \in \mathcal{I}} I) = \bigcap_{I \in \mathcal{I}} \mathbb{V}(I)$ *where $\mathcal{I}$ is an arbitrary set of ideals of R.*

Proof. Exercise. □

Theorem 2.59. *For any ring R, the Zariski topology on* $\mathrm{Spec}(R)$ *satisfies the axioms of a topology given in Definition 2.56.*

Proof. This follows from the above propostition. □

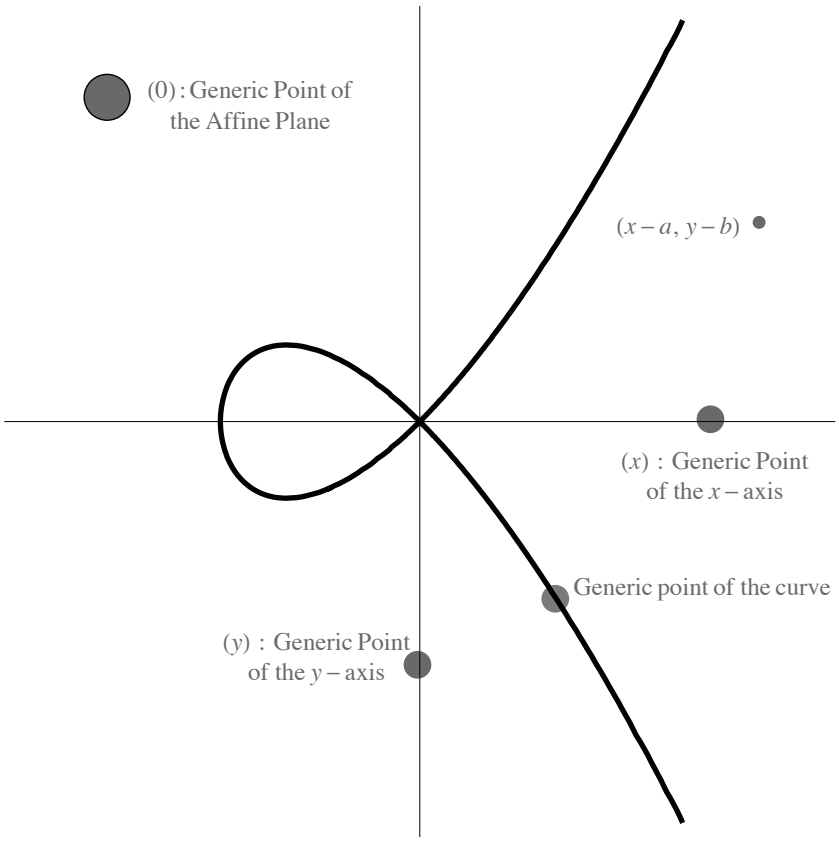
Remark 2.60. Let's consider the case where $R = K[X]$ is an affine algebra and see what these notions represent. I will use the word variety for irreducible algebraic set below.

maximal ideal $\overline{\mathfrak{m}_{\underline{a}}} \in \mathrm{mSpec}(R)$	$\rightsquigarrow$	point $\underline{a} \in X$
prime ideal $\mathfrak{p} = \overline{P} \in \mathrm{Spec}(R)$	$\rightsquigarrow$	generic point of the algebraic set $Y = \mathbb{V}(P) \subseteq X$
closed set $\mathbb{V}(I)$	$\rightsquigarrow$	all subvarieties $Y \subseteq \mathbb{V}(I) \subseteq X$
distinguished open set $D(f)$	$\rightsquigarrow$	all subvarieties $Y \subseteq X$ such that $Y \not\subseteq \mathbb{V}(f)$

So we can think of $\mathrm{mSpec}(R)$ as being the points of X and of $\mathrm{Spec}(R)$ as an enriched version of X where we have added a new "generic point" point for any subvariety of X. Specifically, we call the point $\mathfrak{p} \in \mathrm{Spec}(R)$ the *generic point* of the algebraic subset $V(\mathfrak{p}) \subseteq X$.

In summary, $\mathbb{V}(I)$ contains all the points of the vanishing set $V(I) = X$, but also additional "generic points".

Example 2.61. Here is a picture of $\mathrm{Spec}(K[x, y])$ (from Eisenbud-Harris's book) illustrating the geometric meaning of several primes: the prime (0) is the generic point of $\mathbb{A}^2_K$, the prime ideals which are not maximal are generic points of various curves in the plane, while the maximal ideals $(x - a, y - b)$ correspond to points $(a, b) \in \mathbb{A}^2_K$.



Since (0) is contained in all prime ideals, the only Zariski open set containing the

ideal (0) is $\mathrm{Spec}(R)$, so the "generic point" of X cannon be separated from any other point of $\mathrm{Spec}(R)$ by an open set.

This shows that **the Zariski topology is in general highly non-Hausdorff**.

Example 2.62. For a field K, $\mathrm{Spec}(K) = \{0\}$ consists of just one element so we can think of it as a single point. The functions from a singleton set to K are in bijection with K so this supports our intuition that the spectrum should be a for which K represents the algebraic functions.

For $R = K[x]/(x^2)$, the spectrum also consists of a single point $\mathrm{Spec}(R) = \{(x)\}$. However notice that $R \ncong K$ so this point should be different than the one discussed previously. Indeed if we take $f \in K[x]$ then the image of f in R only remembers the value of $f(0)$, that is the constant term, and the value of the derivative $\partial f/\partial x$ at 0 (this is the coefficient of x in f). Therefore we thing of $\mathrm{Spec}\, R$ as a *fat point*, that is, a point together with a tangent direction (corresponding to dx) so that the functions on this fat point are of the form $a + bx$ with the coefficient a indicating the value at the point and one b indicating the magnitude of a tangent vector.

Next we make Spec into a functor. To do this, we have to apply it to ring homomorphisms.

Definition 2.63 (Induced map on Spec)**.** Given a homomorphism of rings $\varphi : R \to S$, there is an induced map on spectra $\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ given by $\varphi^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$.

The key point is that the preimage of a prime ideal is also prime. We will often write $\mathfrak{p} \cap R$ for $\varphi^{-1}(\mathfrak{p})$, even if the map is not necessarily an inclusion.

Proposition 2.64. *For a ring homomorphism $\varphi : R \to S$ $\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is order preserving and continuous with respect to the Zariski topologies.*

Proof. Exercise. □

Continuity of the induced map makes Spec a functor $\mathrm{Spec} : \langle\langle \mathrm{Rings} \rangle\rangle \to \langle\langle \mathrm{Top} \rangle\rangle$.

Theorem 2.65 (The spec functor)**.** Spec *is a contravariant functor between the categories of rings and topological spaces*

$$\langle\langle \mathit{Rings} \rangle\rangle \xrightarrow{\mathrm{Spec}} \langle\langle \mathit{Top} \rangle\rangle .$$

I will not prove this in detail, but let's see some examples.

Example 2.66. Let $\pi : R \to R/I$ be the (surjective) quotient map. Then the map $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ corresponds to the inclusion of $V(I)$ into $\mathrm{Spec}(R)$, since primes of R/I correspond to primes of R containing I.

Example 2.67. The ring $K[x,y]/(xy)$ gives rise to the topological space

$$X = \mathrm{Spec}(K[x,y]/(xy)) = \{(x), (y), (x, f(y)), (g(x), y) \mid g \in K[x], f \in K[y] \text{ irreducible}\},$$

which is the union of the two coordinate axes in the plane together with all their points. The canonical surjections

$$\pi_1 : K[x,y]/(xy) \to K[x,y]/(y) = K[x].$$

$$\pi_2 : K[x,y]/(xy) \to K[x,y]/(x) = K[y]$$

give rise to the continuous injective maps

$$\iota_1 = \mathrm{Spec}(\pi_1) : \mathrm{Spec}(K[x]) \to X, \qquad (g(x)) \mapsto (g(x), y).$$

$$\iota_2 = \mathrm{Spec}(\pi_2) : \mathrm{Spec}(K[y]) \to X, \qquad (f(y)) \mapsto (x, f(y)).$$

which are the inclusions of the two coordinate axes with their respective points in X.

Notice that the functor Spec of Theorem 2.65 is not an equivalence of categories because example 2.62 illustrates that different rings can yield the same topological space (a point). To remedy this, one must consider instead of topological spaces algebraic schemes, a notion which you may learn about in a course on algebraic geometry. The functor Spec yields a contravariant equivalence between the category of commutative rings and the **category of affine schemes**.

Chapter 3

Primary decomposition

March 1st, 2021

One reason to like noetherian rings is the existence of finite irreducible factorizations.

Recall that an element a of a domain is irreducible if whenever $a = uv$, u or v must be a unit. In Math 818 we proved that in a noetherian ring (e.g. a PID) every element factors as a finite product of irreducible elements. But irreducible factorizations are not unique, famously because of examples like $\mathbb{Z}[\sqrt{-5}]$ where

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We shall look for an analogue of factorization at the level of ideals: say we are working in $\mathbb{Z}$ and we have a prime factorization $a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, with $p_1, \dots, p_n$ distinct (prime hence) irreducible elements. Since $(p_i^{e_i}), (p_j^{e_j})$ are comaximal for $i \neq j$, we can write

$$(a) = (p_1^{e_1})(p_2^{e_2}) \dots (p_n^{e_n}) = (p_1^{e_1}) \cap (p_2^{e_2}) \cap \dots \cap (p_n^{e_n})$$

The second equality holds by the Chinese Remainder Theorem. It turns out that the idea of decomposing ideals by intersections is one that generalizes. We will look for decompositions for ideals in the form of finite intersections of irreducible ideals.

Definition 3.1. Say an ideal I of a ring R is *irreducible* if whenever $I = I_1 \cap I_2$ with I_1, I_2 ideals of I, then $I = I_1$ or $I = I_2$.

An expression $I = I_1 \cap \dots \cap I_n$ is called an *irreducible decomposition* for an ideal I if $I_1, \dots, I_n$ are irreducible ideals.

Example 3.2. Every prime ideal is irreducible. Indeed if $I = I_1 \cap I_2$ and $a \in I \setminus I_1, b \in I \setminus I_2$ then $ab \in I$, contradicting the primality of I.

Similarly to irreducible factorizations, every ideal in a noetherian ring has a finite irreducible decomposition.

Theorem 3.3. *Ler R be a noetherian ring and I and ideal of R. Then there exists a positive integer n and irreducible ideals $I_1, \dots, I_n$ such that*

$$I = I_1 \cap \dots \cap I_n.$$

Proof. If I is irreducible, set $n = 1$ and $I_1 = I$.

Otherwise $I = J_1 \cap J_2$ for some ideals J_1, J_2. If J_1, J_2 are irreducible then we have found an irreducible decomposition. Otherwise continue with decomposing J_1, J_2 as further intersections of ideals. The process of successive decomposition must stop after a finite number of steps otherwise we would have an infinite ascending chain

$$I = \subsetneq J_i \subsetneq \cdots$$

contradicting the noetherian property of R. □

To summarize, our aim is to decompose ideals in a ring R. Further, decomposition should mean that we present them as an intersection of other ideals. However, we still need to answer the following questions:

Question 3.4. *1. What kind of ideals should be allowed in the intersection?*

2. What restrictions should be put on the ring R?

3. Can we expect the decomposition to be unique?

3.1 Primary ideals and primary decompositions

We now look at what makes an ideal irreducible. [1] We'll start with an a priori unrelated notion, which generalizes the class of ideals (p^n), where p is a prime element in a UFD.

Definition 3.5. Let R be a ring. An ideal $Q \subseteq R$ is called *primary* if for all $a, b \in R$ with $ab \in Q$ we have $a \in Q$ or $b^n \in Q$ for some $n \in \mathbb{N}$.

Lemma 3.6. *The radical of a primary ideal is prime.*

Proof. If $\mathfrak{p} = \sqrt{Q}$ with Q primary and $\sqrt{Q} = \mathfrak{p}$ then $ab \in \mathfrak{p}$ implies $a^n b^n \in Q$ for some $n \in \mathbb{N}$ and so some powers of a or b are in Q by the definition of primary. Thus a or b are in $\mathfrak{p}$. □

Definition 3.7. One says that Q is $\mathfrak{p}$-*primary* to indicate that Q is primary and $\sqrt{Q} = \mathfrak{p}$.

Example 3.8.

- Prime ideals are primary.
- In a PID, the primary ideals are the powers of prime ideals i.e. (0) and $(p)^n = (p^n)$ where p is a prime element. (exercise).
- In general, primary ideals need not be powers of prime ideals: Let $Q = (x^2, y)$ and $\mathfrak{p} = (x, y)$ in $R = k[x, y]$. Then Q is P-primary. However, $\mathfrak{p}^2 \subsetneq Q \subsetneq \mathfrak{p}$.

[1] There is a more general theory of irreducible modules, irreducible decomposition for modules, primary modules and primary decomposition for modules, which we skip for the sake of time and because it arises less often in practice.

- Powers of prime ideals need not be primary: Let $R = \frac{k[x,y,z]}{(xy-z^2)}$ and $\mathfrak{p} = (x, z)$. Then $\mathfrak{p}$ is prime but the power $\mathfrak{p}^2 = (x^2, xz, z^2)$ is not primary as $xy = z^2 \in \mathfrak{p}^2$, but neither is x in $\mathfrak{p}^2$ nor any power of y.
- However any power $\mathfrak{m}^n, n \in \mathbb{N}$ of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary (exercise).

March 3, 2021

Here are some an alternate interpretations for primary ideals.

Lemma 3.9. *Let R be a ring and Q an ideal of R. The following are equivalent:*

1. *Q is primary*
2. *every element of R/Q is either a non-zerodivisor or it is nilpotent*

Proof. (1) $\Rightarrow$ (2) Suppose $\overline{a} \in R/Q$ is a zerodivisor. Then $ab \in Q$ for some $b \in R$ such that $b \notin Q$ (that is, $\overline{b} \neq 0$ in R/Q). Because I is assumed primary we obtain that $a^n \in I$ for some $n \in \mathbb{N}$, so $\overline{a}^n = 0$ in R/Q, making $\overline{a}$ nilpotent.

(2) $\Rightarrow$ (1) Suppose $ab \in I$. Then $\overline{ab} = 0$ in R/Q and so either $\overline{b}$ is a non-zerodivisor and thus $a \in Q$ or $\overline{b}$ is nilpotent and then $b^n \in Q$ for some $n \in \mathbb{N}$.

□

The following result clarifies the relationship between irreducible and primary ideals.

Proposition 3.10. *If R is a noetherian ring and I is an irreducible ideal then I is primary.*

Proof. We show that irreducibility implies property (2) of the previous proposition.

Since I is irreducible in R, 0 is an irreducible ideal of $\bar{R} = R/I$. Let $a \in R$ and consider the map $\varphi : \bar{R} \to \bar{R}$ given by $\varphi(\bar{m}) = \overline{a}\bar{m}$.

$$\operatorname{Ker}(\varphi) \subset \operatorname{Ker}(\varphi^2) \subset \cdots$$

forms an ascending chain of ideals of $\bar{R}$. Since R is noetherian, $\bar{R}$ is noetherian. Thus the above chain of submodules stabilizes; that is, there is an integer n such that

$$\operatorname{Ker}(\varphi^n) = \operatorname{Ker}(\varphi^{n+1}) = \operatorname{Ker}(\varphi^{n+2}) = \cdots .$$

Set $g = \varphi^n$. Then $\operatorname{Ker}(g) = \operatorname{Ker}(g^2)$ from which it follows that

$$\operatorname{Im}(g) \cap \operatorname{Ker}(g) = (0).$$

Since (0) is irreducible, either $\operatorname{Im}(g) = (0)$ or $\operatorname{Ker}(g) = (0)$. If $\operatorname{Im}(g) = (0)$, then $\overline{a}$ is nilpotent. If $\operatorname{Ker}(g) = (0)$, then $\operatorname{Ker}(\varphi) = (0)$ and $\overline{a}$ is a non-zerodivisor. □

Remark 3.11. The converse is true in PIDs: every primary ideal of a principal ideal domain is an irreducible ideal. (exercise)

Definition 3.12. For a ring R and ideal I, a *primary decomposition* of I is an expression of the form

$$I = Q_1 \cap \cdots \cap Q_m$$

with each Q_i a primary ideal.

Such a decomposition is *irredundant* if for each i, Q_i does not contain $\bigcap_{j \neq i} Q_j$.

Such a decomposition is *minimal* if I is not the intersection of j primary ideals for any $j < m$. Note that a minimal primary decomposition is automatically irredundant (but not conversely).

Example 3.13. The following are two primary decompositions for an ideal of $K[x, y]$:

$$(x^2, y) \cap (x, y^2) = (x^2, xy, y^2)$$

The decomposition on the left is irredundant, but not minimal. The decomposition on the right is irredundant and minimal.

We come to the existence of primary decompositions in noetherian rings.

Theorem 3.14 (Lasker-Noether primary decomposition theorem)**.** *Every ideal in a noetherian ring has a primary decomposition.*

Proof. Follows from Proposition 3.3 because irreducible decompositions are a special case of primary decompositions by Proposition 3.10. □

March 5, 2021

First let's examine some examples of primary decompositions:

Example 3.15.

$$(x^2, xy) = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y)$$

are two *distinct* minimal primary decompositions for the ideal $(x^2, xy) \subseteq K[x, y]$. Set $Q_1 = (x)$, $Q_2 = (x^2, xy, y^2)$ and $Q_2' = (x^2, y)$ and notice that $\sqrt{Q_1} = \mathfrak{p}_1 = (x)$ and $\sqrt{Q_2} = \sqrt{Q_2'} = \mathfrak{p}_2 = (x, y)$.

Notice some similarities and some differences between the two decompositions

- the radicals of the primary components are the same in both decompositions
- the primary components corresponding the the *minimal* prime $\mathfrak{p}_1$ are the same in both decompositions (see below for the definition of minimal prime)
- the primary components corresponding the the *embedded* prime $\mathfrak{p}_2$ are **not** the same in both decompositions (see below for the definition of embedded prime)

Definition 3.16. A prime ideal $\mathfrak{p}$ is a *minimal prime* of I (or of R/I) if it is a minimal element of $\mathbb{V}(I)$ with respect to containment. The set of minimal primes of I is denoted $\operatorname{Min}(I)$.

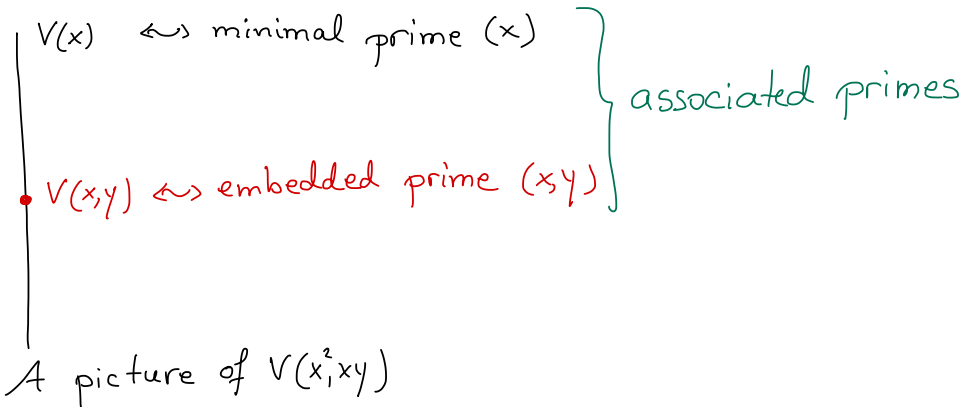
Remark 3.17. One can prove, using Zorn's lemma, that for each ideal I, $\mathrm{Min}(I) \neq \emptyset$. A similar argument shows that every element of $\mathbb{V}(I)$ contains an element of $\mathrm{Min}(I)$.

Example 3.18. For $I = (x^2, xy)$ and for any $\mathfrak{p} \in \mathbb{V}(I), x^2 \in \mathfrak{p}$ it follows that $(x) \subseteq \mathfrak{p}$. Thus (x) is the unique minimal element of $\mathbb{V}(I)$, that is $\mathrm{Min}(I) = \{(x)\}$.

On HW 2, you have shown that $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$. Let's use this to give a geometric interpretation of the decomposition above:

$$V(x^2, xy) = V(x) \cup V(x^2, xy, y^2) = V(x) \cap V(x^2, y)$$

shows the algebraic set $V(x^2, xy)$ as the union of the y-axis ($V(x)$) and the point $(0,0) = V(x^2, xy, y^2) = V(x^2, y) = V(x, y)$. Since the point $(0,0)$ is contained in the y-axis we call it an embedded point and we call $\mathfrak{p}_2 = (x, y)$ an embedded prime.



In general we have a correspondence

minimal primes	=	maximal irreducible algebraic subsets of $V(I)$
embeded primes	=	non-maximal irreducible algebraic subsets of $V(I)$

A fact about radicals:

Lemma 3.19. *For any ideals I and J of the same ring we have $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

Corollary 3.20 (Prime decomposition)**.** *Every radical ideal I in a noetherian ring is an intersection of finitely many prime ideals in* $\mathrm{Min}(I)$.

Proof. From the Lasker-Noether theorem, we have a primary decomposition

$$I = Q_1 \cap \cdots \cap Q_n.$$

Taking radicals yields

$$I = \sqrt{I} = \sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n,$$

where $\mathfrak{p}_i = \sqrt{Q_i}$ are prime ideals. The conclusion about minimal ideals follows by noticing that any non-minimal prime appearing in the decomposition above can be

replaced by a minimal prime that it contains without making the intersection any smaller. To be precise, for each i pick $p_i' \in \mathrm{Min}(I)$ such that $\mathfrak{p}_i' \subseteq \mathfrak{p}_i$. Then

$$I \subseteq \mathfrak{p}_1' \cap \cdots \cap \mathfrak{p}_n' \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = I$$

yields

$$I = \mathfrak{p}_1' \cap \cdots \cap \mathfrak{p}_n'.$$

□

Remark 3.21. The corollary above implies that for a radical ideal in a noetherian ring $I = \cap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}$. On HW 3 you are asked for a different proof of this statement which does not use the noetherian hypothesis.

Example 3.22. The radical ideal (xy) decomposes as $(xy) = (x) \cap (y)$. Notice that this corresponds to the irreducible decomposition of the algebraic set $V(xy) = V(x) \cup V(y)$.

This leads to

A Geometric interpretation for prime decomposition.

Let's apply the prime decomposition theorem to radical ideals in a polynomial ring $R = K[x_1, \ldots, x_n]$. Corollary 3.20 says that

> Every radical ideal $I \subseteq K[x_1, \ldots, x_n]$ is the intersection of finitely many prime ideals $\mathfrak{p}_i \in \mathrm{Min}(I)$
>
> $$I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m.$$

Let's translate this into geometric language using the inclusion reversing correspondence between ideals and algebraic sets. The translation gives a fact proven on HW2:

> Every algebraic subsets X is a finite union of irreducible algebraic subsets X_i:
>
> $$X = X_1 \cup \cdots \cup X_m$$

Moreover the following is true:

> Given a decomposition as above that is iredundant (for all $i \neq j, X_i \not\subseteq X_j$) then the irreducible subvarieties $X_1, \ldots, X_m$ are unique up to ordering.

This would translate algebraically into

> Given a prime decomposition $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$ so that for all $i \neq j$ we have $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ (i.e. the primes appearing in the decomposition are minimal) then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are unique up to ordering.

Before we consider how this uniqueness aspect of the prime decompositions generalizes, we embark into a study of the prime ideals arising as radicals of the primary components in a primary decomposition.

3.2 Associated primes

We next identify the radicals of primary ideals in a primary decomposition. Towards this end, we first define a notion of "associated primes" which are determined by an ideal I and later we show that the radicals of the primary components in an irredundant primary decomposition of I are these associated primes, hence they depend only on I and not on the decomposition.

Definition 3.23. Let R be a ring, and M a module. We say that $\mathfrak{p} \in \operatorname{Spec}(R)$ is an *associated prime* of M if $\mathfrak{p} = \operatorname{Ann}_R(m) = \{r \in R \mid rm = 0\}$ for some $m \in M$. We write $\operatorname{Ass}_R(M)$ for the set of associated primes of M:

$$\operatorname{Ass}_R(M) = \{\operatorname{Ann}_R(m) \mid m \in M\} \cap \operatorname{Spec}(R).$$

If I is an ideal, by the *associated primes* of I we (almost always) mean the associated primes of R/I; but we'll try to write $\operatorname{Ass}_R(R/I)$. Since the annihilator of an element $\overline{r} \in R/I$ is $\operatorname{Ann}_R(\overline{r}) = \{b \in R \mid br \in I\} \stackrel{def}{=} I : r$ we have

$$\operatorname{Ass}_R(R/I) = \{I : r \mid r \in R\} \cap \operatorname{Spec}(R).$$

Lemma 3.24. *Let R be a ring, and M a module. The following are equivalent*

1. *$\mathfrak{p}$ is associated to M*
2. *there is an injective R-module homomorphism $R/\mathfrak{p} \hookrightarrow M$.*

Proof. For (1) $\Rightarrow$ (2)

$$\begin{array}{lcl} \mathfrak{p} \text{ is associated to } M & \iff & \mathfrak{p} = \operatorname{Ann}_R(m) \text{ for some } m \in M \\ & \iff & \mathfrak{p} \text{ is the kernel of the homomorphism } \mu_m : R \to M, r \mapsto rm \\ & \iff & \overline{\mu}_m : R/\mathfrak{p} \hookrightarrow M \text{ is injective.} \end{array}$$

For (2) $\Rightarrow$ (1) notice that any homomorphism $f : R/\mathfrak{p} \hookrightarrow M$ is of the form $f = \overline{\mu}_m$ for $m = f(1)$ and apply the argument above in reverse. □

Example 3.25. If $\mathfrak{p}$ is a prime ideal then $\mathfrak{p} \in \operatorname{Ass}_R(R/\mathfrak{p})$ by using the identity map $R/\mathfrak{p} \hookrightarrow R/\mathfrak{p}$.

Perhaps the most important fact is that associated primes always exist:

Theorem 3.26. *Let R be a ring and M an R-module.*

1. *Every maximal (w.r.t. containment) member of the collection of ideals*

$$\mathcal{S} = \{I \mid I = \operatorname{Ann}_R(m) \text{ for some } 0 \neq m \in M\}.$$

is a prime ideal.

If R is noetherian and $M \neq 0$ then

2. $\mathrm{Ass}_R(M) \neq \emptyset$

3. *The set of zero-divisors of M is the union of the associated primes of M.*

$$\mathcal{D}(M) := \{r \in R \mid rm = 0 \text{ for some } 0 \neq m \in M\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \mathfrak{p}.$$

This subset is not usually an ideal.

Proof. For (1), let $\mathfrak{p}$ be a maximal member of $\mathcal{S}$. Say $\mathfrak{p} = \mathrm{Ann}_R(m)$, for some $m \neq 0$. Note that $\mathfrak{p} \neq R$ since $1 \notin \mathrm{Ann}_R(m)$. Say $rs \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. Then $rsm = 0$ and $sm \neq 0$, and thus $\mathfrak{p} \subseteq \mathfrak{p} + (r) \subseteq \mathrm{Ann}_R(sm) \in \mathcal{S}$. By the maximality of $\mathfrak{p}$, we have $\mathfrak{p} = (r, \mathfrak{p}) = \mathrm{Ann}_R(sm)$. It follows that $r \in \mathfrak{p}$.

For (2), since $M \neq 0$, $\mathcal{S} \neq \emptyset$ and, since we assume R is noetherian, $\mathcal{S}$ has a least one maximal member, which belongs to $\mathrm{Ass}_R(M)$ by (1).

For (3), if $rm = 0$ for some $0 \neq m \in M$, then $\mathrm{Ann}_R(m) \in \mathcal{S}$ and hence it must be contained in a maximal member of $\mathcal{S}$, which belongs to $\mathrm{Ass}_R(M)$ by (1). So $\supseteq$ holds. The other containment is clear from the definitions. (If $r \in \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Ass}_R(M)$, then $\mathfrak{p} = \mathrm{Ann}_R(m)$ for some $m \neq 0$, and so $rm = 0$.) □

The converse of part 1 of the above theorem is not true.

Example 3.27. Consider $R = K[x, y], I = (x^2y, xy^2)$ and $M = R/I$. Then the following three ideals are all prime ideals and members of $\mathcal{S}$

$$\begin{aligned} (x) &= \mathrm{Ann}(y^2) \\ (y) &= \mathrm{Ann}(x^2) \\ (x, y) &= \mathrm{Ann}(xy). \end{aligned}$$

However, (x) and (y) are not maximal in $\mathcal{S}$ w.r.t containment, as they are properly contained in (x, y).

Using the theorem we can give a third equivalent definition for primary ideals

Corollary 3.28. *Q is a $\mathfrak{p}$-primary ideal of a noetherian ring R iff $\mathrm{Ass}_R(R/Q) = \{\mathfrak{p}\}$.*

Proof. Let $\mathfrak{p} = \sqrt{Q}$ and $\mathfrak{q} \in \mathrm{Ass}_R(R/Q)$. Then $\mathfrak{q} = \mathrm{Ann}_R(m)$ for some $m \in R/Q$ implies $Q \subseteq \mathfrak{q}$ and taking radicals gives $\mathfrak{p} \subseteq \mathfrak{q}$.

We have

$$\begin{aligned} Q \text{ is } \mathfrak{p}\text{-primary} &\iff \mathcal{D}(R/Q) = \sqrt{Q} = \mathfrak{p} && (\text{ Lemma 3.9}) \\ &\iff \mathfrak{p} = \textstyle\bigcup_{\mathfrak{q} \in \mathrm{Ass}_R(R/Q)} \mathfrak{q} && (\text{Theorem 3.26 part 3.}) \\ &\iff \mathrm{Ass}_R(R/Q) = \{\mathfrak{p}\}. \end{aligned}$$

The converse statement follows by reversing the arrows above. □

This achieves the goal of showing that the associated primes are exactly the radicals of primary components in the case where the primary decomposition has exactly one component. To extend this to several components we shall study intersections of ideals using short exact sequences. We shall also "zoom in" on one primary component at a time using localization. Thus we need to see how associated primes behave in short exact sequences and under localization

Proposition 3.29 (Associated primes in short exact sequences)**.** *If R is a ring and $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then*

$$\mathrm{Ass}_R(M') \subseteq \mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(M') \cup \mathrm{Ass}_R(M'')$$

If the sequences is split exact, then $\mathrm{Ass}_R(M) = \mathrm{Ass}_R(M') \cup \mathrm{Ass}_R(M'')$. In particular,

$$\mathrm{Ass}_R(M' \oplus M'') = \mathrm{Ass}_R(M') \cup \mathrm{Ass}_R(M'').$$

Proof. For notational simplicity, assume $M' \subseteq M$ and $M'' = M/M'$. For the first containment, recall $\mathfrak{p} \in \mathrm{Ass}_R(M')$ iff there is an R-module injection $R/\mathfrak{p} \hookrightarrow M'$. In this case, since $M' \subseteq M$, $\mathfrak{p} \in \mathrm{Ass}_R(M)$ too.

To prove the second one, say $\mathfrak{p} \in \mathrm{Ass}_R(M)$ so that there is an R-module injection $j : R/\mathfrak{p} \hookrightarrow M$. If the composition $R/\mathfrak{p} \xrightarrow{j} M \twoheadrightarrow M''$ is also injective, then $\mathfrak{p} \in \mathrm{Ass}_R(M'')$. Otherwise, there is a $0 \neq \overline{r} \in R/\mathfrak{p}$ such that $j(\overline{r}) \in M'$. Consider the composition

$$R/\mathfrak{p} \xrightarrow{r} R/\mathfrak{p} \xhookrightarrow{j} M.$$

Since $R/\mathfrak{p}$ is a domain, the first map is also injective, and hence so is the composition, and its image is contained in $R \cdot j(\overline{r}) \subseteq M'$. This proves $\mathfrak{p} \in \mathrm{Ass}_R(M')$.

The final assertion holds since if the sequence is split, then we also have a s.e.s. $0 \to M'' \to M \to M' \to 0$ so that $\mathrm{Ass}_R(M'') \subseteq \mathrm{Ass}_R(M)$ too. □

Corollary 3.30. *If Q_1, Q_2 are $\mathfrak{p}$-primary ideals of a noetherian ring R, then $Q_1 \cap Q_2$ is also $\mathfrak{p}$-primary.*

Proof. We have the short exact sequence

$$0 \to R/Q_1 \cap Q_2 \to R/Q_1 \oplus R/Q_2 \to R/(Q_1 + Q_2) \to 0.$$

Therefore

$$\mathrm{Ass}_R(R/Q_1 \cap Q_2) \subseteq \mathrm{Ass}_R(R/Q_1 \oplus R/Q_2) = \mathrm{Ass}_R(R/Q_1) \cup \mathrm{Ass}_R(R/Q_2) = \{\mathfrak{p}\}$$

shows that $Q_1 \cap Q_2$ is $\mathfrak{p}$-primary by the previous Corollary. □

The previous corollary says that one can consolidate the primary components with the same radical in an irredundant decomposition into *one* primary ideal.

Remark 3.31. A consequence of the above corollary is that if $I = Q_1 \cap \cdots \cap Q_n$, is a minimal primary decomposition, then $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$. We will see later that this condition is equivalent to having a minimal primary decomposition.

3.3 Interlude on localization

Recall that if R is a commutative ring and S is a multiplicatively closed subset of R, then one constructs a new ring called the *localization of R at S* as follows

$$S^{-1}R = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\} / \sim,$$

where $\sim$ is the equivalence relation $\frac{r}{s} \sim \frac{r'}{s'} \iff \exists s'' \in S$ such that $s''(rs' - r's) = 0$. Moreover, localization at S is a functor

$$S^{-1}(-) : \langle\langle R\text{-modules} \rangle\rangle \to \left\langle\left\langle S^{-1}R\text{-modules} \right\rangle\right\rangle$$

defined on objects by

$$M \mapsto S^{-1}M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\} / \sim$$

and on morphisms by

$$(f : M \to N) \mapsto \left(S^{-1}f : S^{-1}M \to S^{-1}N, \quad m/s \mapsto f(m)/s \right).$$

Example 3.32 (Most important localizations)**.** Let R be a ring.

1. For $f \in R$ and $S = \{1, f, f^2, f^3, \ldots\}$, we usually write R_f or $R[\frac{1}{f}]$ for $S^{-1}R$.
2. For $\mathfrak{p} \subset R$ prime, we generally write $R_{\mathfrak{p}}$ for $(R \setminus \mathfrak{p})^{-1}R$.
3. When W is the set of nonzerodivisors on R, we call $W^{-1}R$ the *total ring of fractions* of R. When R is a domain, this is just the fraction field of R.

Remark 3.33. In Math 901 we proved:

- The extension of scalars functor $S^{-1}R \otimes_R -$ along the canonical map $\phi : R \to S^{-1}R, \phi(r) = \frac{r}{1}$ is isomorphic to the localization functor $S^{-1}(-)$ by means of the family of isomorphisms of $S^{-1}R$-modules

$$\eta_M : S^{-1}R \otimes_R M \xrightarrow{\cong} S^{-1}M, \frac{r}{s} \otimes m \mapsto \frac{rm}{s}.$$

- Localization is an exact functor and $S^{-1}R$ is a flat R-module.

We will be interested on the correspondence between ideals of R and $S^{-1}R$ under the localization map $\phi : R \to S^{-1}R, r \mapsto \frac{r}{1}$. Note that ϕ is injective if and only if S contains no zero divisors.

First, a more general setup:

Definition 3.34. If $\phi : A \to B$ is a ring homomorphism, then for any ideal I of B,

$$\phi^{-1}(I) = \{a \in A \mid \phi(a) \in I\}.$$

is an ideal of A. This is called the *contraction* of I along ϕ. If $\phi : R \to S^{-1}R$ maps $r \mapsto \frac{r}{1}$ from some multiplicatively closed set S, then for an ideal I of $S^{-1}R$ we write $I \cap R$ for the contraction $\phi^{-1}(I)$.

Definition 3.35. If $\phi : A \to B$ is a ring homomorphism, then for an ideal J of A, we write

$$JB = \left\{ \sum_{i=1}^{n} \phi(a_i) b_i \mid a_i \in J, b_i \in B \right\}.$$

Then JB is an ideal of B (it's the smallest ideal of B containing the image of J under ϕ in fact.) The ideal JB is called the *extension* of J along ϕ.

Remark 3.36. If R is a ring, J and ideal of R, and S a multiplicatively closed set then

$$JS^{-1}R = \left\{ \sum_{i=1}^{n} \frac{j_i}{s_i} \mid j_i \in J, s_i \in S \right\} = \left\{ \frac{j}{s} \mid j \in J, s \in S \right\} = S^{-1}J.$$

March 12, 2020

Proposition 3.37. *Let R be a commutative ring and $S \subseteq R$ a mcs. Let $\phi : R \to S^{-1}R$ denote the canonical ring map (sending r to $\frac{r}{1}$).*

1. *For any ideal I of $S^{-1}R$, we have $(I \cap R)S^{-1}R = I$ (i.e, extension $\circ$ contraction along ϕ is the identity mapping on the set of ideals of $S^{-1}R$).*
2. *The contraction function*

   $$\phi^* : \{\text{ideals of } S^{-1}R\} \to \{\text{ideals of } R\}, I \mapsto \phi^{-1}(I) = I \cap R$$

   is injective and it preserves inclusions and intersections of ideals.
3. *An ideal J belongs to the image of ϕ^* if and only if the following property holds: whenever $s \in S$ and $r \in R$ are such that $sr \in J$, then $r \in J$.*
4. *In particular, ϕ^* induces an isomorphism of posets*

   $$\operatorname{Spec}(S^{-1}R) \overset{\text{bijection}}{\longleftrightarrow} \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \cap S = \emptyset\}.$$

Proof. For (1), suppose $a \in I \cap R$, $r \in R$, $s \in S$. Then $\frac{a}{1}\frac{r}{s} \in I$ and so $\subseteq$ holds. If $\frac{r}{s} \in I$, then $\frac{r}{1} \in I$ and hence $r \in I \cap R$. Thus $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} \in (I \cap R)S^{-1}R$, so that $\supseteq$ also holds.

The first part of (2) is an immediate consequence of (1), since (1) shows that extension is the left inverse of contraction. The remaining claims of (2) are clear from the definitions.

For (3), if $J = I \cap R$, then $JS^{-1}R = I$ by (1). If $rs \in J$, then $\frac{rs}{1} \in JS^{-1}R = I$ and hence $\frac{rs}{1} \cdot \frac{1}{s} = \frac{r}{1} \in I$ so that $r \in J$.

Conversely, if J satisfies the given property we set $I = JS^{-1}R$ and we show $I \cap R = J$. The containment $JS^{-1}R \cap R \supseteq J$ is clear. If $a \in I \cap R$, then $\frac{a}{1} = \frac{b}{s}$ for some $b \in J$ and $s \in S$. Thus $s'(as - b) = 0$ for some $s \in S$ and hence $(s's)a = s'b =\in J$. By assumption $a \in J$ and so $a \in J$.

For (4), if $\mathfrak{p} \in \operatorname{Spec}(R)$, then the condition that $sr \in \mathfrak{p}$ implies $r \in \mathfrak{p}$ is equivalent to $S \cap \mathfrak{p} = \emptyset$. So (4) follows from (3). □

Corollary 3.38. *For any commutative ring R and $\mathfrak{p} \in \operatorname{Spec}(R)$, there is an isomorphism of posets*

$$\operatorname{Spec}(R_{\mathfrak{p}}) \overset{\text{bijection}}{\longleftrightarrow} \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \subseteq \mathfrak{p}\} = \operatorname{Spec}(R) \setminus \mathbb{V}(\mathfrak{p}).$$

In particular, $R_{\mathfrak{p}}$ is a local ring*; i.e., it has a unique maximal ideal*

$$\mathfrak{p}R_{\mathfrak{p}} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}.$$

Example 3.39. For any prime integer p, the ring $\mathbb{Z}_{(p)}$ has just two prime ideals: the 0 ideal and the ideal $\{\frac{np}{m} \mid p \nmid m\}$, which is generated by $\frac{p}{1}$.

Example 3.40. $\operatorname{Spec}(R[1/f])$ is in bijective correspondence with the collection of prime ideals of R that do *not* contain f. This is what's called a *principal open set* of the Zariski topology on $\operatorname{Spec}(R)$.

Remark 3.41. Proposition 3.37 does *not* state that contraction and extension are inverse to each other when applied to all ideals of R. In particular extension followed by contraction may not be identity as shown by the following example.

Example 3.42. Consider $R = \mathbb{Z}$ and its localization at $S = \mathbb{Z}\setminus\{0\}$, namely $S^{-1}R = \mathbb{Q}$. Now an ideal (n) of $\mathbb{Z}$ extends to

$$(n)\mathbb{Q} = \begin{cases} (0) & \text{if } n = 0 \\ \mathbb{Q} & \text{if } n \neq 0 \end{cases} \qquad \text{hence} \qquad (n)\mathbb{Q} \cap \mathbb{Z} = \begin{cases} (0) & \text{if } n = 0 \\ \mathbb{Z} & \text{if } n \neq 0. \end{cases}$$

We see that $(n)\mathbb{Q} \cap \mathbb{Z} \neq (n)$ if $n \neq (0)$.

March 15, 2021

However extension followed by contraction is identity when applied to primary ideals.

Lemma 3.43. *An ideal Q is $\mathfrak{p}$-primary if and only if $\sqrt{Q} = \mathfrak{p}$ and $QR_{\mathfrak{p}} \cap R = Q$.*

Proof. For the forward direction:

$$\begin{aligned} r \in QR_{\mathfrak{p}} \cap R &\iff \frac{r}{1} = \frac{q}{s} \text{ for some } q \in Q, s, s \in R \setminus \mathfrak{p} \\ &\iff rs'' \in Q \text{ for some } s'' \in R \setminus \mathfrak{p} \Rightarrow r \in Q. \end{aligned}$$

For the last implication we have use the definition of $\mathfrak{p}$-primary and the fact that $s'' \in R \setminus \mathfrak{p}$ implies that all the powers of s'' are also in $R \setminus \mathfrak{p}$. □

Next we look at how associated primes behave under localization.

Theorem 3.44 (Associated primes localize)**.** *Let R be a noetherian ring, S a multiplicatively closed subset of R and M an R-module. Then the associated primes of $S^{-1}M$ are*

$$\operatorname{Ass}_{S^{-1}R}(S^{-1}M) = \{S^{-1}\mathfrak{q} \in \operatorname{Ass}_R(M) \mid \mathfrak{q} \cap S = \emptyset\}.$$

Proof. Recall from Proposition 3.37 (4) that the map $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$ induces a bijection

$$\operatorname{Spec}(S^{-1}R) \overset{\text{bijective}}{\longleftrightarrow} \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \cap S = \emptyset\}$$

with inverse given by $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$. To prove the Theorem, we just need to show each of these functions restrict to maps between the indicated subsets.

If $\mathfrak{q} \in \operatorname{Ass}_R(M)$ and $\mathfrak{q} \cap S = \emptyset$, then there is an injective R-module map

$$i : R/\mathfrak{q} \hookrightarrow M.$$

Since localization is exact, this gives an injection

$$S^{-1}R/S^{-1}\mathfrak{q} \cong S^{-1}(R/\mathfrak{q}) \hookrightarrow S^{-1}M$$

of $S^{-1}R$-modules, and so $S^{-1}\mathfrak{q} \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M)$.

If $\mathfrak{p} \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M)$, then there is an injective $S^{-1}R$-module map

$$j : S^{-1}R/\mathfrak{p} \hookrightarrow S^{-1}M$$

Set $\mathfrak{q} = \phi^{-1}(\mathfrak{p}) \in \operatorname{Spec}(R)$ so that $\mathfrak{p} = S^{-1}\mathfrak{q}$.

Since R is noetherian, $R/\mathfrak{q}$ is finitely presented as an R-module and thus we have

$$S^{-1}\operatorname{Hom}_R(R/\mathfrak{q}, M) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}R/\mathfrak{p}, S^{-1}M).$$

(We have also used the canonical isomorphism $S^{-1}(R/\mathfrak{q}) \cong S^{-1}R/S^{-1}\mathfrak{q}$ here.)

In particular, this gives us that the map j has the form $\frac{g}{s}$ for some R-module map $g : R/\mathfrak{q} \to M$ and $s \in S$. I claim g is an injection: If $g(\overline{r}) = 0$, then since $\frac{g}{s}$ is injective we must have $\frac{\overline{r}}{1} = 0$ in $S^{-1}(R/\mathfrak{q})$. But then $\overline{r} = 0$ since every element of S is a non-zero-divisor on $R/\mathfrak{q}$. This proves $\mathfrak{q} \in \operatorname{Ass}_R(M)$. □

Corollary 3.45. *Taking $S = R \setminus \mathfrak{p}$ gives a bijective correspondence*

$$\mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) = \{\mathfrak{q}R_\mathfrak{p} \mid \mathfrak{q} \in \mathrm{Ass}_R(M), \mathfrak{q} \subseteq \mathfrak{p}\}.$$

Corollary 3.46 (Primary decompositions localize)**.** *Suppose R is a noetherian ring, I is an ideal, $I = Q_1 \cap \cdots \cap Q_m$ is a primary decomposition of I, and S is a multiplicatively closed subset of R. Set $\mathfrak{p}_i = \sqrt{Q_i}$ and assume further that the list $Q_1, \ldots, Q_m$ is ordered so that $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are all the primes such that $\mathfrak{p}_i \cap S = \emptyset$ if and only if $1 \leq t \leq m$. Then*

$$S^{-1}I = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_t$$

is a primary decomposition of the ideal $S^{-1}I$ in $S^{-1}R$.

Proof. For ideals J_1 and J_2 in R we have

$$S^{-1}(J_1 \cap J_2) = S^{-1}J_1 \cap S^{-1}J_2.$$

For each $i > t$, $\mathfrak{p}_i \cap S \neq \emptyset$ and since $\sqrt{Q_i} = \mathfrak{p}_i$, it follows that $S \cap Q_i \neq \emptyset$ and hence $S^{-1}Q_i = S^{-1}R$. From these facts, we get that

$$S^{-1}I = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_t \tag{3.1}$$

For $1 \leq i \leq t$, by Theorem 3.44 (associated primes localize) we have

$$\mathrm{Ass}_{S^{-1}R}(S^{-1}R/S^{-1}Q_i) = \{S^{-1}\mathfrak{p}_i\}$$

and thus $S^{-1}Q_i$ is a $S^{-1}\mathfrak{p}_i$-primary ideal in the ring $S^{-1}R$. Thus (3.1) is indeed a primary decomposition. □

Remark 3.47. The proof of the previous statement establishes the following claim about localizations of primary ideals: for a $\mathfrak{p}$-primary ideal Q

$$S^{-1}Q = \begin{cases} S^{-1}R & \text{if } \mathfrak{p} \cap S \neq \emptyset \\ S^{-1}\mathfrak{p} - \text{primary} & \text{if } \mathfrak{p} \cap S = \emptyset. \end{cases}$$

Example 3.48. For the ideal $I = (x^2y, xy^2)$ of $R = K[x, y]$ with primary decomposition

$$(x^2y, xy^2) = (x) \cap (y) \cap (x^2, y^2)$$

we have the following localized primary decompositions

$$\begin{aligned} I_{(x)} &= (x)R_{(x)} \\ I_{(y)} &= (y)R_{(y)} \\ I_{(x,y)} &= (x)R_{(x,y)} \cap (y)R_{(x,y)} \cap (x, y)R_{(x,y)}. \end{aligned}$$

3.4 Uniqueness aspects of primary decomposition

We first show that the radicals of the primary components in all irredundant decompositions of a fixed ideal I are the same and are uniquely determined by I. You may want to review Definition 3.12 for the meaning of irredundant and minimal primary decomposition.

Theorem 3.49 (First uniqueness theorem for primary decomposition)**.** *Let R be a noetherian ring and I an ideal. Suppose*

$$I = Q_1 \cap \cdots \cap Q_m$$

is a primary decomposition of I and set $\mathfrak{p}_i = \sqrt{Q_i}$ so that Q_i is $\mathfrak{p}_i$-primary for each i. Then:

1. $\mathrm{Ass}_R(R/I) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$.
2. *If the intersection is irredundant, then $\mathrm{Ass}_R(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ (there might be repetitions in the list $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$).*
3. *If the intersection is minimal, then $\mathrm{Ass}_R(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ and there are no repetitions in the list $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. In particular, $|Ass_R(R/I)|$ is the number of primary ideals in any minimal primary decomposition of I.*

Proof. For (1) the canonical map

$$R/I \to R/Q_1 \oplus \cdots \oplus R/Q_m,$$

given by $x + I \mapsto (x + Q_1, \ldots, x + Q_m)$ is injective. So

$$\mathrm{Ass}_R(R/I) \subseteq \mathrm{Ass}_R(R/Q_1 \oplus \cdots \oplus R/Q_m) = \bigcup_i \mathrm{Ass}_R(R/Q_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}.$$

For (2), for each i the canonical map

$$L := \left(\bigcap_{j \neq i} Q_j\right)/I \hookrightarrow R/Q_i, \quad x + I \mapsto x + Q_i$$

is injective and (since the intersection is non-redundant) $L \neq 0$. So we have

$$\emptyset \neq \mathrm{Ass}_R(L) \subseteq \mathrm{Ass}_R(R/Q_i) = \{\mathfrak{p}_i\}$$

and hence $\mathrm{Ass}_R(L) = \{\mathfrak{p}_i\}$. On the other hand, L is clearly a submodule of R/I too, and hence $\mathrm{Ass}_R(R/I) \supseteq \mathrm{Ass}_R(L)$.

For (3), note that if the intersection is minimal, it's certainly irredundant. The conclusion follows from (2) and Remark 3.31. □

Corollary 3.50. *Given a primary decomposition $I = Q_1 \cap \cdots \cap Q_m$, the following are equivalent*

1. *the decomposition is minimal*
2. $|\operatorname{Ass}_R(R/I)| = m$
3. *the decomposition is irredundant and $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$.*

Proof. (1) $\Leftrightarrow$ (2) follows from part (3) of Theorem 3.49.

(1) $\Rightarrow$ (3) follows from the definition of minimal primary decomposition and Remark 3.31.

For (3) $\Rightarrow$ (1) we see from (2) of tof Theorem 3.49 that $\operatorname{Ass}_R(R/I) = \{\mathfrak{p}_1, \ldots \mathfrak{p}_m\}$, where $\mathfrak{p}_i = \sqrt{Q_i}$. Since the $\mathfrak{p}_i$'s are distinct, $|\operatorname{Ass}_R(R/I)| = m$, hence the decomposition is minimal because (2) $\Rightarrow$ (1). □

Recall that the minimal primes of I coincide the minimal members of the set of primes that contain I. The minimal primary components of an I *are* unique:

Theorem 3.51 (Second uniqueness theorem for primary decompositions)**.** *The primary ideals in a minimal primary decomposition that correspond to minimal primes are unique. That is, if $I = Q_1 \cap \cdots \cap Q_m$ and $I = Q'_1 \cap \cdots \cap Q'_m$ are two minimal primary decompositions of the same ideal I, ordered so that $\sqrt{Q_i} = \sqrt{Q'_i} = \mathfrak{p}_i$ for all i and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are the minimal primes of I, then $Q_i = Q'_i$ for $1 \leq i \leq t$.*

Proof. Fix $1 \leq i \leq t$. For all $j \neq i$, we have $\mathfrak{p}_j \cap (R \setminus \mathfrak{p}_i) \neq \emptyset$ since $\mathfrak{p}_i$ is minimal and hence $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$. Corollary 3.46 and the remark following it thus give

$$IR_{\mathfrak{p}_i} = Q_i R_{\mathfrak{p}_i} \quad \text{and} \quad IR_{\mathfrak{p}_i} = Q'_i R_{\mathfrak{p}_i}.$$

Taking contractions through the localization map $\phi : R \to R_{\mathfrak{p}_i}$ and using Lemma 3.43 we see that $Q_i = Q_i R_{\mathfrak{p}_i} \cap R = Q'_i R_{\mathfrak{p}_i} \cap R = Q'_i$. □

Look back at Example 3.15 for an illustration of this theorem.

Remark 3.52. In the setting of Corollary 3.46, a minimal primary decomposition localizes to a minimal primary decomposition and an irredundant primary decomposition localizes to an irredundant primary decomposition.

Specifically, suppose R is a noetherian ring, I is an ideal,

$$I = Q_1 \cap \cdots \cap Q_m \tag{3.2}$$

is a primary decomposition of I, and S is a multiplicatively closed subset of R. Set $\mathfrak{p}_i = \sqrt{Q_i}$ and assume further that the list $Q_1, \ldots, Q_m$ is ordered so that $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are all the primes such that $\mathfrak{p}_i \cap S = \emptyset$ if and only if $1 \leq t \leq m$. Then we know

$$S^{-1}I = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_t \tag{3.3}$$

is a primary decomposition of the ideal $S^{-1}I$ in $S^{-1}R$. Moreover, if (3.2) is minimal then (3.3) is minimal and if (3.2) is irredundant then (3.3) is irredundant.

Indeed if (3.2) is minimal then $\mathrm{Ass}_R(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ and by Theorem 3.44 $\mathrm{Ass}_R(S^{-1}R/S^{-1}I) = \{S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_t\}$ and there are no repetitions in the latter list. Thus (3.3) is minimal.

If (3.2) is irredundant, let $1 \leq i \leq t$ and take $a \in \bigcap_{j \neq i} Q_j \backslash Q_i$. Then $\frac{a}{1} \in \bigcap_{j \neq i} S^{-1}Q_j$ but $\frac{a}{1} \notin S^{-1}Q_i$ since $\frac{a}{1} \in S^{-1}Q_i$ would mean $a \in S^{-1}Q_i \cap R = Q_i$ (this equality is similar to Lemma 3.43 and uses that $S \subseteq R \setminus \mathfrak{p}_i$.)

Chapter 4

Dimension theory I

In linear algebra it is common to talk about the dimension of a vector space. This corresponds to our geometric intuition that if V is an n-dimensional K-vector space then $V \cong \mathbb{A}^n_K$ is geometrically the n-dimensional space.

Question 4.1. *What should the dimension of a ring be?*

We want to create a notion of dimension for rings which matches our geometric intuition in the sense that, for example, the coordinate ring of $\mathbb{A}^n_K$, which is $K[x_1, \ldots, x_n]$ should have dimension n.

However there are spaces which are much more complicated than $\mathbb{A}^n_K$. Let's take for example a copy of $\mathbb{A}^2_K$ union a copy of $\mathbb{A}^1_K$. The coordinate ring for an algebraic set of this form is, for example, $R = K[x, y, z]/(z) \cap (x, y) = K[x, y, z]/(xz, yz)$. What should be the dimension of this ring? There are two competing answers: 1 or 2. Shortly we will describe this situation by saying that R is not equidimensional. Globally, the dimension of R should be 2 because the 2-dimensional component cannot be ignored. However, we get a better understanding of the geometric features if we study the dimension of R locally, at each of its points.

This leads to considering local rings of the form $R_{\mathfrak{m}}$, where $\mathfrak{m}$ is a maximal ideal. There are three plausible ways to define the dimension of such a local ring:

1. *Dimension is the measured by length of chains of primes (irreducible varieties).*

   Specifically, say that $\{\underline{a}\} = X_0 \subsetneq X_1 \subsetneq X_2 \cdots \subsetneq X_d$ is a chain of varieties containing $\underline{a}$. Then our intuition says that the dimension of these varieties has to increase as we go along the chain, i.e. $\dim(X_0) < \dim(X_1) < \cdots < \dim(X_d)$. If we want to make this chain as long as possible, then it is intuitive that the dimension of the varieties involved should only increase by 1 at each step and so $\dim(X_i) = i$ for $0 \leq i \leq d$. We need to stop when we have reached the dimension of the ambient space, and so we declare $\dim R_{\mathfrak{m}} = d$ where d is the maximum integer such that we can find a chain of varieties as above, or equivalently a chain of primes $\mathfrak{p}_d \subsetneq \cdots \subsetneq \mathfrak{p}_0 = \mathfrak{m}$.

2. *Dimension is measured by the number of equations it takes to define a point.*

   Recall that a point in $\mathbb{A}^n_K$ corresponds to a maximal ideal $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ and notice that the number of generators of $\mathfrak{m}$ is $n = \dim(K[x_1, \ldots, x_n])$.

   To generalize this notion of dimension to arbitrary rings, simply set $\dim R_{\mathfrak{m}}$ to be the cardinality of a minimal generating set of $\mathfrak{m}$. Already, the well definedness of this approach poses problems, but we will prove Nakayama's Lemma which says that all minimal generating sets have the same cardinality, making this well defined. If $\underline{a} = Z(m)$ is a smooth point then this definition works beautifully, but we run into problems with singular points.

   For example consider $R = K[x, y]/(xy)$ and $\mathfrak{m} = (x, y)$. Then R is the coordinate ring of the union of the x and y axes so our geometric intuition says that R should have dimension 1, but $\mathfrak{m}$ is not principal. However there is a principal ideal $(x-y)$ of R with the same radical as $\mathfrak{m}$, so $Z(x - y) = Z(\mathfrak{m})$. In fact it can be observed that $(x - y)$ is $\mathfrak{m}$-primary and we revise our definition to say that the dimension is the minimum number of generators of an $\mathfrak{m}$-primary ideal.

3. *Dimension is the measured by the polynomial order of growth of a neighborhood of a point.*

   Say R is the coordinate ring of a variety X and look at measuring the size of a ball centered at $\underline{a} \in X$. If X consists of a discrete set of points then the only "small" ball around $\underline{a}$ is $\underline{a}$ and its size is constant. If a"small" ball centered at $\underline{a}$ looks like an interval (1-dimensional) then its length ($2r$) grows linearly with the radius of the ball, r. If a"small" ball centered at $\underline{a}$ looks like a disc (2-dimensional), then its area πr^2 grows quadratically with the radius of the sphere. If a"small" ball centered at $\underline{a}$ looks like a sphere (3-dimensional), then its volume $\frac{4}{3}\pi r^3$ grows as a polynomial of degree 3 in the radius of the sphere.

   So we will say that $R_{\mathfrak{m}}$ has dimension d if size of a small neighborhood of $\mathfrak{m}$ is a polynomial of order d. We will model these neighborhoods as vector spaces $\mathfrak{m}^r/\mathfrak{m}^{r+1}$ over the field $R/\mathfrak{m}$ and we will measure their size as the vector space dimension $\dim_{R/\mathfrak{m}}(\mathfrak{m}^r/\mathfrak{m}^{r+1})$.

We will spend a good amount of time understanding how to make these definitions rigorous algebraically. The main theorem of dimension theory will be that these three competing definitions for dimension actually agree!

March 19, 2020

4.1 Krull dimension

Definition 4.2. The *Krull dimension* (often just called dimension) of a commutative ring R, written $\dim(R)$, is defined to be

$$\dim(R) = \sup\{d \mid \exists \text{ a strictly increasing chain of prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d\}.$$

We will agree that the dimension of the zero ring is -1, by convention.

Definition 4.3. A chain of primes as above is *saturated* if for each i, there is no $\mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{p}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}_{i+1}$. One can equivalently define $\dim(R)$ as the supremum of the lengths of saturated chains of primes of R.

Example 4.4. 1. The dimension of a field is zero.

2. A ring is zero-dimensional if and only if every minimal prime of (0) is maximal.

3. A domain has Krull dimension 1 if and only if every nonzero prime ideal is maximal. Applying, (2), the ring of integers $\mathbb{Z}$ has dimension one, since there is one minimal prime (0) and every other prime is maximal. Likewise, any PID that is not a field has dimension one.

4. It follows from the definition that if K is a field, then

$$\dim(K[x_1, \ldots, x_d]) \geq d,$$

since there is a saturated chain of primes

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d).$$

We will show eventually that $\dim(K[x_1, \ldots, x_d]) = d$. We accept this fact for now as being true for the purpose of computing examples. One can easily deduce the case $d = 1$, i.e. $\dim(K[x]) = 1$ form (3) above, since this ring is a PID.

Remark 4.5. The definition for the dimension of $K[x_1, \ldots, x_d]$ can be equivalently stated as the supremum of the lengths of strictly increasing chains of irreducible algebraic subsets of the form

$$X_0 \subsetneq \cdots \subsetneq X_d \subseteq \mathbb{A}^n_k.$$

Clearly, we may assume take X_0 to be a single point and $X_d = \mathbb{A}^n_k$ in finding this supremum.

Remark 4.6. The notion of dimension is most meaningful for noetherian rings, although

- there are non-noetherian rings of finite Krull dimension. I leave it as an exercise to find an example.
- **there are noetherian rings of infinite Krull dimension**. This was shown in a famous example due to Nagata presented below.

Example 4.7 (Nagata)**.** Let $R = K[x_1, x_2, \ldots]$. R is clearly infinite-dimensional, but is noetherian. Let

$$W = R \setminus ((x_1) \cup (x_2, x_3) \cup (x_4, x_5, x_6) \cdots)$$

and $S = W^{-1}R$. This ring has primes of arbitrarily large height, given by the images of those primes we cut out from W. Thus, it has infinite dimension by Proposition 4.9 part 4. The work is to show that this ring is noetherian. We omit this argument here.

To aid in computing dimension we make the following related definition

Definition 4.8. The *height* of a prime ideal $\mathfrak{p}$ of a ring R is the supremum of the lengths of (saturated) chains of primes in R that end in $\mathfrak{p}$, in symbols

$$\text{height}(p) = \sup\{h \mid \exists \text{ a strictly increasing chain of prime ideals } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}\}.$$

The *height* of an ideal I is the infimum of the heights of the primes containing I

$$\text{height}(I) = \inf\{\text{height}(\mathfrak{p}) \mid \mathfrak{p} \in V(I)\} = \inf\{\text{height}(\mathfrak{p}) \mid \mathfrak{p} \in \text{Min}(I)\}.$$

To get a feel for these definitions, we make a sequence of easy observations.

Proposition 4.9 (Properties of dimension and height)**.** *1. Dimension and height are isomorphism invariants.*

2. *A prime has height zero if and only if it is a minimal prime of the 0 ideal.*
3. $\dim(R) = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \text{Spec}(R)\} = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \text{Min}(0)\}$.
4. $\dim(R) = \sup\{\text{height}(\mathfrak{p}) \mid \mathfrak{p} \in \text{Spec}(R)\} = \sup\{\text{height}(\mathfrak{m}) \mid \mathfrak{m} \in \text{mSpec}(R)\}$.
5. *If I is an ideal, then* $\dim(R/I)$ *is the supremum of the lengths of (saturated) chains of primes of R, $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$, with each $\mathfrak{p}_i \in V(I)$.*
6. *If I is an ideal,* $\dim(R/I) + \text{height}(I) \leq \dim(R)$.
7. *If S is a multiplicative set, then* $\dim(S^{-1}R) \leq \dim(R)$.
8. *If $\mathfrak{p}$ is prime, then* $\text{height}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$.

Proof. Exercise. □

Let's analyze our example of a copy of $\mathbb{A}^2_K$ union a copy of $\mathbb{A}^1_K$ algebraically.

Example 4.10. The ring $R = \frac{k[x,y,z]}{(xz,yz)}$ has dimension 2.

We will show this using the machinery developed above. First notice that in $k[x,y,z]$ we have the primary decomposition $(xz, yz) = (x,y) \cap (z)$. This leads in R to the primary decomposition $(\bar{0}) = (\bar{x}, \bar{y}) \cap (\bar{z})$. Thus $\text{Min}(0) = \{(x,y),(z)\}$. According to Proposition 4.9 (3), we have

$$\begin{aligned} \dim(R) &= \max\left\{\dim \frac{R}{(\bar{x},\bar{y})}, \dim \frac{R}{(\bar{z})}\right\} \\ &= \max\left\{\dim K[z], \dim K[x,y]\right\} \\ &= \max\{1,2\} = 2. \end{aligned}$$

We can write down an explicit chain of primes of R of length 2:

$$(\bar{z}) \subsetneq (\bar{z},\bar{x}) \subsetneq (\bar{z},\bar{x},\bar{y}).$$

Remark 4.11. The previous example illustrates the principle that the dimension of an algebraic set is the maximum of the dimensions of its irreducible components. Indeed, Proposition 4.9 (3) applied to an affine ring $R = K[x_1, \ldots, x_n]/I$ gives that

$$\dim(R) = \max\{\dim(R/\mathfrak{p}_i) \mid \mathfrak{p}_i \in \operatorname{Min}(I)\}.$$

March 22, 2021

I want to discuss property (6) of Proposition 4.9 in more detail. It says:

Proposition 4.9 (6) If I is an ideal, $\dim(R/I) + \operatorname{height}(I) \leq \dim(R)$.

Proof. The case when $I = P$ is a prime ideal:

By definition of height, we can find a chain of primes of length $\operatorname{height}(P)$ that are all contained in P. We can also find a chain of primes of length $\dim(R/P)$ in R/P. By the lattice isomorphism theorem, this corresponds to a chain of primes in $\mathbb{V}(P)$ of length $\dim(R/P)$ in R/P. Putting the two chains together (largest ideal of the first chain will coincide with the smallest ideal of the second chain), we have a chain of primes of R of length $\dim(R/I) + \operatorname{height}(I)$ and the conclusion follows by definition of $\dim(R)$.

The case when I is an arbitrary ideal:

If $\dim(R/I) = \infty$ then there are chains of primes in $\operatorname{Spec}(R)$ of arbitrary lengths by the lattice isomorphism theorem and then also $\dim(R) = \infty$.

Assume now that $\dim(R/I) < \infty$. Let $\dim(R/I) = \ell$ and takea chain of primes of maximum length in $\operatorname{Spec}(R/I)$ corresponds by the lattice isomorphism theorem to the chain of primes $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_\ell$ with $P_i \in \mathbb{V}(I)$. I claim that $\dim(R/P_0) = \ell$. To establish this claim, note that the chain we wrote guarantees $\dim(R/P_0) \geq \ell$. If $\dim(R/P_0) > \ell$ then we could find a longer chain of primes in $\operatorname{Spec}(R/P_0)$ which would yield a longer chain of primes in $\mathbb{V}(I)$, contradicting that $\dim(R/I) = \ell$.

To finish, observe that $\operatorname{height}(I) \leq \operatorname{height}(P_0)$ by definition of height. Now we can conclude using the former case that

$$\dim(R/I) + \operatorname{height}(I) \leq \dim(R/P_0) + \operatorname{height}(P_0) \leq \dim(R).$$

□

Here is an example which shows that **the inequality** $\dim(R/I) + \operatorname{height}(I) \leq \dim(R)$ **can fail to be an equality**.

Example 4.12. Let $R = \mathbb{Z}_{(2)}[x]$ and consider $\mathfrak{p} = (2x - 1)$. I claim $\mathfrak{p}$ is a prime of height 1. To see this, recall that $\operatorname{height}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$ and notice that since $2 \in R \setminus \mathfrak{p}$ we have

$$\dim R_{\mathfrak{p}} = (\mathbb{Z}_{(2)}[x])_{(2x-1)} = \mathbb{Q}[x]_{(2x-1)}$$

so $\operatorname{height}(\mathfrak{p}) = \dim R_{\mathfrak{p}} = \dim \mathbb{Q}[x]_{(2x-1)} = \operatorname{height}((2x-1)\mathbb{Q}[x]) = 1$.

Moreover, $R/\mathfrak{p} \cong \mathbb{Q}$, so $\dim(R/\mathfrak{p}) = 0$, and therefore $\dim(R/\mathfrak{p}) + \operatorname{height}(\mathfrak{p}) = 1$ whereas $\dim R \geq 2$ as attested by the chain $(0) \subsetneq (2) \subsetneq (2, x)$. In fact, $\dim R = 2$, but I won't justify this.

Definition 4.13. A ring is *catenary* if for every pair of primes $\mathfrak{q} \supseteq \mathfrak{p}$ in R, every saturated chain of primes $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{q}$ has the same length.

The poset of ideals of an catenary ring is a *ranked poset* in the sense one would encounter in combinatorics, where the rank function is the height of an ideal.

It is difficult to come up with examples of rings that are not catenary, but they do exist. Nagata (1956) gave the first example of a noetherian non-catenary ring in the paper *On the chain problem on prime ideals*.

4.2 Chains of primes in integral extensions

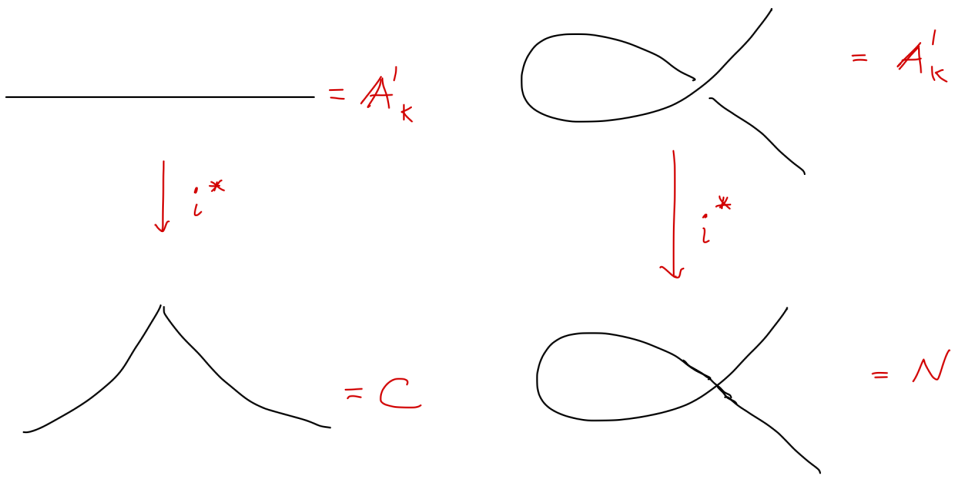
Recall that a ring map $i : A \hookrightarrow B$ of commutative rings is called *module-finite* if B is finitely generated as an A-module.

Recall that a ring map $i : A \hookrightarrow B$ of commutative rings is called *integral* if for all $b \in B$, b is a root of some monic polynomial equation with coefficients in $i(A)$.

Recall that if i is module-finite, then i is integral. The converse holds if i is algebra-finite (Theorem 1.44).

Example 4.14. Think about two typical example of integral injection that we have encountered:

- $K[t^2, t^3] \hookrightarrow K[t]$. This corresponds at the level of algebraic sets to $\mathbb{A}^1_K \twoheadrightarrow C$, where C is the cuspidal curve $C = V(x^3 - y^2) \subseteq \mathbb{A}^2_K$ of Example 2.40.
- $K[t^2-1, t^3-t] \hookrightarrow K[t]$. This corresponds at the level of algebraic sets to $\mathbb{A}^1_K \twoheadrightarrow N$, where N is the nodal cubic of Example 2.41.



Notice some common properties of these morphisms of algebraic sets:

- they are surjective,
- the preimage of each point of the codomain, called the fiber, is a *finite* set of points in the domain. The fibers are not necessarily all of the same cardinality.
- the geometric objects involved all have the same dimension (intuitively, curves have dimension 1).

We will see that the above properties are satisfied by the map on spectra induced by an integral injection.

Before we talk about primes, let's discuss some properties of integral extensions.

March 24, 2021

Lemma 4.15. *Suppose $i : A \hookrightarrow B$ is an integral injection.*

1. *If J is an ideal of B and $I = i^{-1}(J)$ then $A/I \hookrightarrow B/J$ is an integral injection.*
2. *Is S is a multiplicatively closed subset of A then $S^{-1}A \hookrightarrow S^{-1}B$ is an integral injection.*
3. *If B, and hence A, are domains, then A is a field $\iff$ B is a field.*

Proof. I will only record the proof of (3).

" $\Rightarrow$ " If $0 \neq b \in B$, then consider the equation of smallest positive degree it satisfies

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0, a_i \in A.$$

We have $a_n \neq 0$ since otherwise the equation above would factor yielding an integral dependence relation of smaller degree since B is a domain. Since $a_n \neq 0$, a_n is a unit in A, hence also in B. Then we rewrite the equation above as

$$b(b^{n-1} + a_1 b^{n-1} + \cdots + a_{n-1})(-a_n^{-1}) = 1$$

to see that b is invertible in B.

" $\Leftarrow$ " If $0 \neq a \in A$, then it has an inverse $a^{-1} \in B$. We have to show $a^{-1} \in A$. Now a^{-1} stisfies an equation of integral dependence

$$a^{-n} + a_1 a^{-n+1} + \cdots + a_n = 0, a_i \in A.$$

Multiply by a^{n-1} to see $a^{-1} = -(a_1 + \cdots + a_n a^{n-1}) \in A$. □

We now study correspondences between primes in an injective integral extensions which will help explain the properties we have listed above.

Theorem 4.16 (Cohen-Seidenberg)**.** *Suppose $i : A \hookrightarrow B$ is an integral injection.*

1. *(Lying Over Theorem) Given a prime ideal $\mathfrak{p}$ of A, there is a prime ideal $\mathfrak{q}$ of B such that $i^{-1}(\mathfrak{q}) = \mathfrak{p}$.*

   In other words, the induced map $i^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a surjection.

2. *(Going Up Theorem) Given an inclusion $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ of primes ideals of A and a prime ideal $\mathfrak{q}_1$ of B such that $i^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$, there exists a prime ideal $\mathfrak{q}_2$ of B such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $i^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$. In a picture:*

$$\begin{array}{ccc} \mathfrak{q}_1 & \subseteq & \exists\ \mathfrak{q}_2 \\ \downarrow & & \downarrow \\ \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

3. *(Incomparability) There are no inclusions among the prime ideals of B that lie over a given prime of A: if $i^{-1}(\mathfrak{q}_1) = i^{-1}(\mathfrak{q}_2)$ and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

   In other words, each fiber of the map $i^* : \mathrm{Spec}(B) \to Spec(A)$ is a discrete poset.

Proof. (Very technical point: We may assume A, and hence B, is not the zero ring, since if $A = 0$, all the assertions are vacuously true.)

For Lying Over, we first reduce to the case when A is local and $\mathfrak{p}$ is its unique maximal ideal. Let $S = A \setminus \mathfrak{p}$. Since localization is exact, by Lemma 4.15 the induced map $A_\mathfrak{p} = S^{-1}A \to S^{-1}B$ is also an integral injection. Now we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\quad i \quad} & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ S^{-1}A = A_\mathfrak{p} & \longrightarrow & S^{-1}B \end{array}$$

Let $\mathfrak{m}$ be a maximal ideal of $S^{-1}B$. Then $\mathfrak{m} \cap A_\mathfrak{p}$ is a maximal ideal of $A_\mathfrak{p}$ by Lemma 4.15 (1) and (3) since there is an induced integral injection $A_\mathfrak{p}/\mathfrak{m} \cap A_\mathfrak{p} \hookrightarrow S^{-1}B/\mathfrak{m}$ and the right hand side is a field, so the left hand side must be a field as well. But since $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$ we have $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$.

Set $\mathfrak{q} = \beta^{-1}(\mathfrak{m})$. Commutativity of the diagram above yields

$$i^{-1}(\mathfrak{q}) = i^{-1}(\beta^{-1}(\mathfrak{m})) = \alpha^{-1}(\mathfrak{m} \cap A_\mathfrak{p}) = \alpha^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p},$$

so $\mathfrak{q} \in \mathrm{Spec}(B)$ is a prime ideal lying over $\mathfrak{p}$.

For Going Up, note that the induced map $\bar{i} : A/\mathfrak{p}_1 \to B/\mathfrak{q}_1$ is also an integral injection by Lemma 4.15. Appyling Lying Over to $\mathfrak{p}_2/\mathfrak{p}_1$ gives the existence of a prime ideal of the form $\mathfrak{q}_2/\mathfrak{q}_1$ such that $i^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$.

Now for Incomparability. Set $S = A \setminus \mathfrak{p}$. By Lemma 4.15 $j : S^{-1}A \hookrightarrow S^{-1}B$ is integral and $j^{-1}(\mathfrak{q}_1 S^{-1}B) = j^{-1}(\mathfrak{q}_2 S^{-1}B) = \mathfrak{p}S^{-1}A = \mathfrak{p}A_\mathfrak{p}$. As in Lying over we consider the induced integral injection $\bar{j} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \hookrightarrow S^{-1}B/\mathfrak{q}_i S^{-1}B = S^{-1}(B/\mathfrak{q}_i)$. Since the domain of $\bar{j}$ is a field and its target is a domain, we see that by Lemma 4.15

(3) that the codomain is a field as well, thus $\mathfrak{q}_i S^{-1}B$ are two maximal ideals satisfying the containment $\mathfrak{q}_1 S^{-1}B \subseteq \mathfrak{q}_2 S^{-1}B$. This shows that $\mathfrak{q}_1 S^{-1}B = \mathfrak{q}_2 S^{-1}B$ and since $q_i \cap S = \emptyset$ and q_i are prime we deduce that $\mathfrak{q}_1 = \mathfrak{q}_2$.

□

One far-reaching application of this theorem is that one can relate the dimensions of the rings involved in an injective integral extension.

Corollary 4.17. *If $A \hookrightarrow B$ is an integral injection, then* $\dim(A) = \dim(B)$.

Proof. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d$ be any strictly ascending chain in $\mathrm{Spec}(A)$. By the Lying Over/Going Up Theorem, there is a chain $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_d$ in $\mathrm{Spec}(B)$ with $i^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$ for all i. This proves $\dim(A) \leq \dim(B)$.

Now let $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_d$ be any strictly ascending chain in $\mathrm{Spec}(B)$. By incomparability, $i^{-1}(\mathfrak{q}_0) \subset \cdots \subset i^{-1}(\mathfrak{q}_d)$ is a strictly ascending chain in $\mathrm{Spec}(A)$, and thus $\dim(B) \leq \dim(A)$. □

March 26, 2021

Example 4.18. Consider $R = K[x,y]/(y^2 - x(x-1)(x+1))$. The inclusion map $K[x] \hookrightarrow R$ is integral and so $\dim(R) = \dim(K[x]) = 1$.

We now prepare to prove a theorem that goes the opposite way from Going Up and thus bears the name of Going Down, which corresponds to a picture of this form:

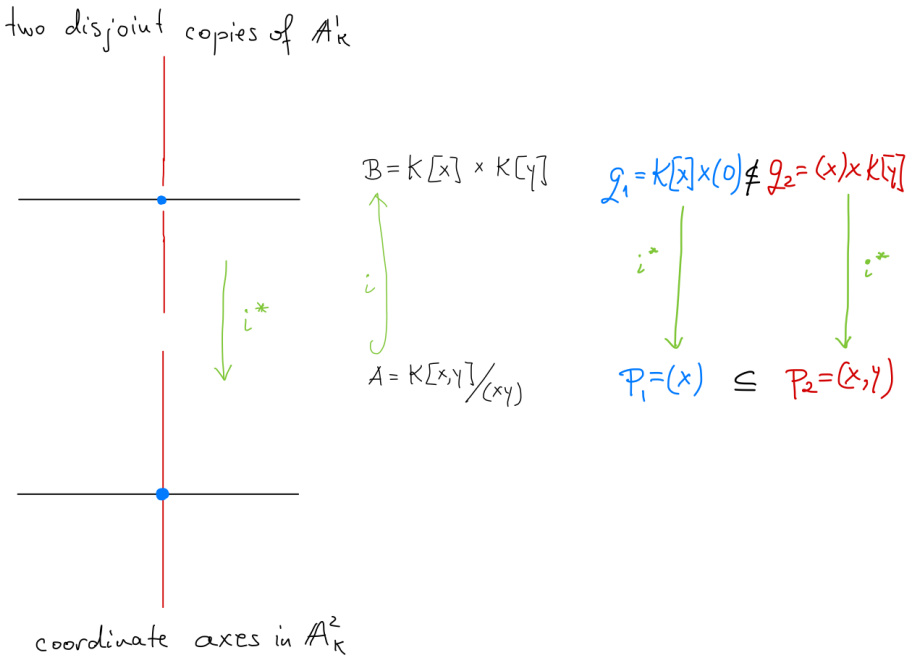
$$\begin{array}{ccc} \exists \mathfrak{q}_1 & \subseteq & \mathfrak{q}_2 \\ \downarrow & & \downarrow \\ \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

Example 4.19. We show that we cannot expect Going Down to hold for arbitrary integral extensions.

Indeed, let $i : A = K[x,y]/(xy) \hookrightarrow B = K[x] \times K[y]$ be the ring homomorphism that takes $f(x,y) \mapsto (f(x,0), f(0,y))$. Then this is integral since we can show each of the K-algebra generators of B are integral over A: both $(1,0)$ and $(0,1)$ satisfy $t^2 - (1,1)t = 0$, with $(1,1) \in i(A)$.

Now choose $\mathfrak{p}_1 = (x) \subseteq \mathfrak{p}_2 = (x,y)$ and $\mathfrak{q}_2 = (x) \times K[y]$. The only prime lying over $\mathfrak{p}_1 = (x)$ is $\mathfrak{q}_1 = K[x] \times (0)$, but $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$. This is because the algebraic set with coordinate ring B consists of two components, $V(\mathfrak{q}_2)$ lies in one of them whereas $V(\mathfrak{q}_1)$ lies in the other component of B; see the figure below.

We see from the example above that we need additional hypotheses for Going Down to hold. In particular, we will want B (hence also A) to be a domain, so that it does not break up into irreducible components. Even for an integral injection of integral domains Going Down may fails, so we need to add additional conditions based on integral closure.



Definition 4.20. A domain is *normal* if it is integrally closed in its field of fractions.

Example 4.21.

- All fields are normal domains.
- Any UFD is normal (same proof as in Example 1.39).
- In particular, $K[x_1, \ldots, x_n]$ is a normal domain if K is a field.

Theorem 4.22 (Going down)**.** *Suppose that A is a normal domain, B is a domain, and $i : A \hookrightarrow B$ is an integral injection. Then, for every $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ in $\operatorname{Spec}(A)$ and $\mathfrak{q}_2$ in $\operatorname{Spec}(B)$ with $i^{-1}(\mathfrak{q}_2) = \mathfrak{p}_2$, there is some $\mathfrak{q}_1 \in \operatorname{Spec}(B)$ with $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $i^{-1}(\mathfrak{q}_1) = \mathfrak{p}_1$. In a picture:*

$$\begin{array}{ccc} \exists \mathfrak{q}_1 & \subseteq & \mathfrak{q}_2 \\ \downarrow & & \downarrow \\ \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

Proof. Omitted in the interest of time. □

Corollary 4.23. *If A is a normal domain, B is a domain, and $A \hookrightarrow B$ is an integral injection, then $\operatorname{height}(\mathfrak{q}) = \operatorname{height}(\mathfrak{q} \cap A)$ for any $\mathfrak{q} \in \operatorname{Spec}(B)$.*

Proof. Set $\mathfrak{p} = \mathfrak{q} \cap A$.

We see that $\operatorname{height}(\mathfrak{q}) \leq \operatorname{height}(\mathfrak{p})$ by taking a chain of primes in $\operatorname{Spec}(B)$ ending with $\mathfrak{q}$, intersecting each with A and using Incomparability to see that the length of the chain remains the same.

To see that that height($\mathfrak{q}$) $\geq$ height($\mathfrak{p}$) take a chain of length height($\mathfrak{p}$) of ideals in Spec(A) ending with $\mathfrak{p}$, and apply Going Down to get a chain just as long that goes up to $\mathfrak{q}$. (Note that the the ideals in the latter chain must be distinct since their contractions in the first chain are distinct.) □

4.3 Noether normalization and the dimension of affine domains

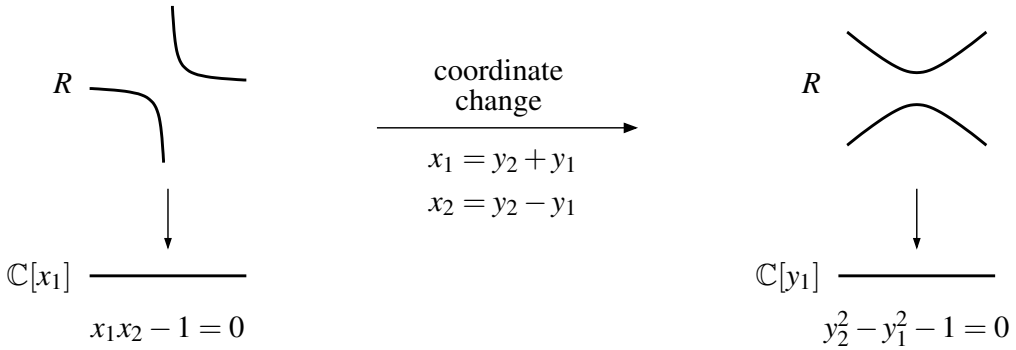
Recall our toy application of Corollary 4.17 for computing dimension using

$$K[x] \hookrightarrow R = K[x, y]/(y^2 - x(x-1)(x+1)).$$

The integral nature of the extension above is granted by the fact that we quotiented by a monic polynomial in y. We show that we can in fact one can rewrite any set of polynomials in this form.

Example 4.24. (Idea behind Noether normalization) Let $R = K[x_1, x_2]/(x_1x_2 - 1)$ be the coordinate ring of the algebraic set $X = V(x_1x_2 - 1) \subset \mathbb{A}^2_K$. We can see from the figure below on the left that R is not integral (and hence not module-finite) over $A = K[x_1]$; this is easily seen geometrically since this map does not satisfy the Lying Over property for the origin.

It is easy to change the situation however by a linear coordinate transformation: if we set e. g. $x_1 = y_2 + y_1$ and $x_2 = y_2 - y_1$ then we can write R also as $R = K[y_1, y_2]/(y_2 - y_2 - 1)$, and now R is integral, hence module-finite, over $A' = C[y_1]$ since the polynomial $y_2 - y_2 - 1$ is monic in y_2. Geometrically, the coordinate transformation has tilted the algebraic set X as in the picture above on the right so that e. g. the Lying Over property now obviously holds. Note that this is not special to the particular transformation that we have chosen; in fact, almost any linear coordinate change would have worked to achieve this goal.



We could have also worked with the coordinate transformation $x_1 = y_1 + y_1^2, x_2 = y_2$ to get that $R \cong K[y_1, y_2]/(y_2^3 + y_1y_2 - 1)$ is integral over $A = K[y_1]$. This type of transformation is explained below.

Lemma 4.25 (Making a pure-power leading term)**.** *Let K be a field, and $f \in R = K[x_1, \ldots, x_n]$ be a polynomial of degree less than N. The A-algebra automorphism of R given by $\phi(x_i) = x_i + x_n^{N^{n-i}}$ for $i < n$ and $\phi(x_n) = x_n$ maps f to a polynomial that, viewed as a polynomial in x_n with coefficients in $K[x_1, \ldots, x_{n-1}]$, has leading term cx_n^a for some $c \in K^\times$, $a \in \mathbb{N}$.*

Proof. The map ϕ sends a monomial $dx_1^{a_1} \cdots x_n^{a_n}$ to a polynomial with unique highest degree term $dx_n^{a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1}N + a_n}$. Since each a_i is less than N in each monomial, the map

$$(a_1, \ldots, a_n) \mapsto a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1}N + a_n$$

is injective when restricted to the set of exponent tuples; thus, none of the terms can cancel. We find that the leading term is of the promised form.

□

Theorem 4.26 (Noether Normalization)**.** *Let K be a field, and R be a finitely generated K-algebra. Then, there are $x_1, \ldots, x_d \in R$ algebraically independent over K such that $K[x_1, \ldots, x_d] \hookrightarrow R$ is module-finite.*

Proof. We proceed by induction on the number of generators n of R over K, with the case $n = 0$ being trivial (in that case $R = K$ and $K \hookrightarrow R$ is module-finite).

Now, suppose that we know the result for K-algebras generated by at most $n-1$ elements. If $R = K[r_1, \ldots, r_n]$, with $r_1, \ldots, r_n$ algebraically independent over A, we are done by setting $d = n$ and $x_i = r_i$.

Assume now that there is some relation on the r's: there is some $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \setminus \{0\}$ such that $f(r_1, \ldots, r_n) = 0$. By taking an A-algebra automorphism (changing the generators of R as in Lemma 4.25), we can assume that f has leading term cx_n^N (in terms of x_n) for some $c \in K^\times$. Then, $c^{-1}f$ is monic in x_n and $c^{-1}f$ is an equation of integral dependence for r_n' over $K[r_1', \ldots, r_{n-1}']$.

Thus $R' = K[r_1', \ldots, r_{n-1}'] \hookrightarrow R = K[r_1, \ldots, r_n]$ is integral. By the inductive hypothesis there exist $x_1, \ldots, x_d \in R'$ that are algebraically independent over K so that $K[x_1, \ldots, x_d] \hookrightarrow R'$ is module-finite. Thus we have two module-finite injections

$$K[x_1, \ldots, x_d] \hookrightarrow R' \hookrightarrow R.$$

Transitivity of module-finite gives that $K[x_1, \ldots, x_d] \hookrightarrow R$ is module-finite. □

In view of the above theorem we define a Noether normalization as follows:

Definition 4.27. Let R be a finitely generated K-algebra for some field K. Then a *Noether normalization* of R is a polynomial ring $A = K[x_1, \ldots, x_t] \subseteq R$ such that $x_1, \ldots, x_t$ are algebraically independent over K and R is module-finite over A.

We can now relate the notion of Noether normalization to that of Krull dimension.

Theorem 4.28. *Let R be a finitely generated domain over a field K and let $A = K[z_1, \ldots, z_d]$ be a Noether normalization for R. Then the length of any saturated chain of primes from 0 to any maximal ideal $\mathfrak{m}$ of R is d.*

In particular, $\dim(R) = d$ *is the number of algebraically independent elements in any Noether normalization for R.*

Moreover, $\dim(R) = \mathrm{trdeg}_K(\mathrm{Frac}(R))$.

March 31, 2021

Proof. The proof is by induction on d.

When $d = 0$, R is a domain that is integral over a field, hence R is a field by Lemma 4.15 (3). Since all fields have Krull dimension 0, the claim holds.

For $d > 0$, pick a saturated chain

$$0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k = \mathfrak{m}$$

and consider the contractions to $A = K[z_1, \ldots, z_d]$:

$$0 \subsetneq \mathfrak{p}_1 = \mathfrak{q}_1 \cap A \subsetneq \cdots \subsetneq \mathfrak{p}_k = \mathfrak{q}_k \cap A.$$

By the saturated condition, $\mathrm{height}(\mathfrak{q}_1) = 1$, and therefore $\mathrm{height}(\mathfrak{p}_1) = 1$, by Corollary 4.23. Since A is a UFD, $\mathfrak{p}_1 = (f)$ for some prime element f. To see this, note that since $\mathfrak{p}_1 \neq 0$ there is some $0 \neq g \in \mathfrak{p}_1$, and primeness implies one of the irreducible factors of g, call it f, is contained in $\mathfrak{p}_1$. Since f is irreducible, hence prime, there is a chain of prime ideals $0 \subsetneq (f) \subseteq \mathfrak{p}_1$ and since $\mathrm{height}(\mathfrak{p}_1) = 1$ we must have $\mathfrak{p}_1 = (f)$.

After a change of variables, we can assume that f is monic in z_d over $K[z_1, \ldots, z_{d-1}]$, so that $K[z_1, \ldots, z_{d-1}] \subseteq A$ is module-finite. Then Now, $K[z_1, \ldots, z_{d-1}] \subseteq A/(f) \subseteq R/\mathfrak{q}_1$ are module-finite, in other words $K[z_1, \ldots, z_{d-1}]$ is a Noether normalization for the domain $R/\mathfrak{q}_1$. Since

$$0 = \mathfrak{q}_1/\mathfrak{q}_1 \subsetneq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k/\mathfrak{q}_1 = \mathfrak{m}/\mathfrak{q}_1$$

is a saturated chain in the affine domain $R/\mathfrak{q}_1$ to the maximal ideal $\mathfrak{m}/\mathfrak{q}_1$, we can apply the induction hypothesis to say that the chain above in $R/\mathfrak{q}_1$ has length $d - 1$, so $k - 1 = d - 1$, and $k = d$.

This finishes the proof about length of saturated chains in R. The statement that $\dim(R) = d$ follows from what was established regarding length of chains from 0 to $\mathfrak{m} \in \mathrm{mSpec}(R)$, since any chain of primes in R of longest possible length must start with 0 and end with a maximal ideal.

Finally, if $A = K[z_1, \ldots, z_d]$ is a Noether normalization for R, then notice that the inclusion $K \hookrightarrow \mathrm{Frac}(R)$ factors into a purely transcendental extension $K \hookrightarrow \mathrm{Frac}(A) = K(z_1, \ldots, z_d)$, and an algebraic extension $\mathrm{Frac}(A) \hookrightarrow \mathrm{Frac}(R)$, whence by Remark 2.5 (3) we have

$$\mathrm{trdeg}_K(\mathrm{Frac}(R)) = \mathrm{trdeg}_K(\mathrm{Frac}(A)) = \mathrm{trdeg}_K(K(z_1, \ldots, z_d)) = d = \dim(A) = \dim(R).$$

□

We finally come to the promised formula for the dimension of a polynomial ring.

Corollary 4.29. *The dimension of the polynomial ring $K[x_1, \ldots, x_d]$ is d.*

Proof. $A = R = K[x_1, \ldots, x_d] \hookrightarrow R$ is a Noether normalization. □

Here are some more nice properties for the dimension of a finitely generated K-algebra:

Corollary 4.30. *If R is a finitely generated K-algebra then* $\dim(R)$ *is finite.*

Proof. This follows from the theorem regarding the existence of Noether normalizations 4.26 since if $K[x_1, \ldots, x_d] \hookrightarrow R$ is a Noether normalization then $\dim(R) = d < \infty$. Moreover, proof of the Noether normalization theorem yields that $\dim(R)$ is at most the number of K-algebra generators of R. □

Corollary 4.31. *If R is a finitely generated K-algebra domain then* $\operatorname{height}(\mathfrak{m}) = \dim R$ *for every maximal ideal $\mathfrak{m}$ of R.*

Remark 4.32. For arbitrary rings R the above corollary does nor hold: the ideal $\mathfrak{p}$ in Example 4.12 is maximal with $\operatorname{height}(\mathfrak{p}) = 1 < \dim(R) = 2$.

Chapter 5

Dimension theory II

March 30, 2020

5.1 Local rings and Nakayama's Lemma

Before getting more into dimension theory, we need to discuss local rings and an important and famous theorem applicable to them.

Definition 5.1. A *local ring* is a ring that has a unique maximal ideal. We write $(R, \mathfrak{m}, k)$ to denote that R is a local ring, $\mathfrak{m}$ is the unique maximal ideal of R and $R/\mathfrak{m} = k$ is the *residue field* of R

An equivalent characterization for local rings is the following:

Lemma 5.2. *R is local if and only if the set of non units of R forms an ideal (this ideal must then be the unique maximal ideal).*

Remark 5.3. The zero ring is not local because it has no maximal ideal.

Example 5.4. Examples of local rings include:

- All fields are local with (0) as the maximal ideal.
- The ring $\mathbb{Z}/(p^n)$ is local with maximal ideal (p).
- The power series ring with coefficients in a field K, $K[[x_1, \ldots, x_n]]$, whose elements are (possible infinite) sums of monomials in the variables $x_1, \ldots, x_n$ is local. Indeed, a power series has an inverse if and only if its constant term is nonzero. The complement of this set of units is the maximal ideal $(x_1, \ldots, x_n)$.
- Any localization $R_{\mathfrak{p}}$, of a ring R at a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.

- A local ring we will often encounter is $K[x_1, \ldots, x_d]_{(x_1,\ldots,x_d)}$. We can consider this as the ring of rational functions that in lowest terms have a denominator with nonzero constant term. (We can talk about lowest terms since the polynomial ring is a UFD.)
- Extending the following example, for any any ideal $I \subseteq K[x_1, \ldots, x_n]$ and any point $\underline{a} \in Z(I)$ with maximal ideal $\mathfrak{m}_{\underline{a}}$ we have a local ring of the form

  $$(K[x_1, \ldots, x_d]/I)_{\mathfrak{m}_{\underline{a}}}.$$

  If K is algebraically closed and I is a radical ideal, then $K[x_1, \ldots, x_d]/I = K[X]$ is the coordinate ring of the affine variety $X = Z(I)$, and we call

  $$\mathcal{O}_{X,\underline{a}} = K[X]_{\mathfrak{m}_{\underline{a}}} = (K[x_1, \ldots, x_d]/I)_{\mathfrak{m}_{\underline{a}}}$$

  the *local ring of the point* $\underline{a} \in X$. The elements of this ring can be interpreted as those rational functions (fractions with polynomial numerator and denominator) which are well defined as set theoretic functions $\{\underline{a}\} \to K$, that is the denominator is nonzero when evaluated at $\underline{a}$.

April 2, 2021

We now proceed to Nakayama's Lemma (a.k.a. NAK). There are a number of statements that go under this name, including and most importantly Theorem 5.5 and Corollary 5.7 below.

Theorem 5.5 (Nakayama's Lemma)**.** *Let R be a commutative ring and J an ideal that is contained in all the maximal ideals of R. Let M be a finitely generated R-module. Let JM denote the submodule of M generated by $\{jm \mid j \in J, m \in \mathfrak{m}\}$. If $JM = M$, then $M = 0$.*

In particular, if $(R, \mathfrak{m})$ is local and M is a finitely generated module with $M = JM$ for some ideal J of R, then $M = 0$.

Proof. Assume $JM = M$.

Let M be generated by $y_1, \ldots, y_k$ as an R-module. It follows that JM is generated by $\{ay_i \mid a \in J, 1 \leq i \leq k\}$ and so, since $y_i \in M = JM$ for all i, we have

$$\begin{aligned} y_1 &= a_{1,1}y_1 + \cdots + a_{k,1}y_k \\ y_2 &= a_{1,2}y_1 + \cdots + a_{k,2}y_k \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ y_k &= a_{1,k}y_1 + \cdots + a_{k,k}y_k \end{aligned}$$

for some $a_{i,j} \in J$. Let $T = (a_{i,j})_{1 \leq i,j \leq k}$ and let $v \in M^{\oplus k}$ be the column vector $\begin{bmatrix} y_1, \ldots, y_k \end{bmatrix}^T$. The equations above give $Tv = v$ or equivalently $(I_k - T)v = 0$. Now, since all the entries of T are in J, we have

$$\det(I_k - T) = 1 + \text{element of } J.$$

For any maximal ideal $\mathfrak{m}$, we have $J \subseteq \mathfrak{m}$ and hence $\det(I_k - T) \notin \mathfrak{m}$. It follows that $\det(I_k - T)$ is a unit in R. By the determinant trick in Lemma 1.42, we have

$$\det(I_k - T)v = \mathrm{adj(I_k - T)}(I_k - T)v = \mathrm{adj(I_k - T)}0 = 0$$

and since $\det(I_k - T)$ is a unit it follows that $v = 0$. That means $y_i = 0$ for all i and hence $M = 0$. □

Before stating a corollary of NAK that also goes by the name of Nakayama's Lemma, I wish to make a remark about how we can obtain vector spaces from modules over local rings.

Remark 5.6. Let $(R, \mathfrak{m}, k)$ be a local ring, and let M be an R-module. Then $M/\mathfrak{m}M$ is an $R/\mathfrak{m} = k$ vector space.

Indeed tensoring the following short exact sequence by M

$$0 \to \mathfrak{m} \to R \to k \to 0$$

yields a right exact sequence

$$\mathfrak{m} \otimes_R M \to R \otimes_R M \to k \otimes_R M \to 0.$$

Now we know that $R \otimes_R M \cong M$. Substituting this into the sequence above gives

$$\mathfrak{m} \otimes_R M \to M \to k \otimes_R M \to 0.$$

where the first map sends $t \otimes m \mapsto tm$, thus the image of this map is $\mathfrak{m}M$. Therefore we obtain an exact sequence

$$0 \to \mathfrak{m}M \to M \to k \otimes_R M \to 0$$

and the isomorphism $k \otimes_R M \cong M/\mathfrak{m}M$ follows. Because k is a k-module, $k \otimes_R M$ is a k vector space and thus so is $M/\mathfrak{m}M$.

Corollary 5.7. *Let $(R, \mathfrak{m}, k)$ be a local ring, and let M be a finitely generated R-module. For $m_1, \ldots, m_s \in M$ with images $\overline{m_1}, \ldots, \overline{m_s} \in M/\mathfrak{m}M$*

$$m_1, \ldots, m_s \text{ generate } M \iff \overline{m_1}, \ldots, \overline{m_s} \text{ generate } M/\mathfrak{m}M.$$

Thus, any generating set for M consists of at least $\dim_k(M/\mathfrak{m}M)$ elements.

Proof. Consider the submodule $N = m_1R + \cdots + m_sR \subseteq M$. We have by NAK that

$$\begin{aligned} M/N = 0 &\iff M/N = \mathfrak{m}(M/N) \iff M/N = (\mathfrak{m}M + N)/N \iff M = \mathfrak{m}M + N \\ &\iff M/\mathfrak{m}M = (\mathfrak{m}M + N)/\mathfrak{m}M \\ &\iff M/\mathfrak{m}M \text{ is generated by the image of } N, \text{that is by } \overline{m_1}, \ldots, \overline{m_s}. \end{aligned}$$

□

Definition 5.8. Let $(R, \mathfrak{m})$ be a local ring, and M a finitely generated module. A set of elements $\{m_1, \ldots, m_t\}$ is a *minimal generating set* of M if the images $\overline{m_1}, \ldots, \overline{m_s}$ of $m_1, \ldots, m_t$ form a basis for the $R/\mathfrak{m} = k$ vector space $M/\mathfrak{m}M$.

It is a consequence of the above definition that all minimal generating sets of M have the same cardinality. We denote this by $\mu(M)$ and refer to it as the *number of minimal generators* of M.

In fact there are two other equivalent definitions for a minimal generating set:

Lemma 5.9. *Let $(R, \mathfrak{m})$ be a local ring, and M a finitely generated module with elements $m_1, \ldots, m_s \in M$. The following are equivalent:*

1. *the images of $m_1, \ldots, m_t$ form a basis for the $R/\mathfrak{m} = k$ vector space $M/\mathfrak{m}M$.*
2. *the set $\{m_1, \ldots, m_s\}$ generates M and is minimal with respect to containment among all sets of generators for M*
3. *the set $\{m_1, \ldots, m_s\}$ generates M and has minimal cardinality among all sets of generators of M.*

Proof. Homework. □

April 5, 2021

5.2 Artinian rings and finite length modules

To prepare for our next big theorems in dimension theory, we need to understand the structure of zero-dimensional noetherian rings. To spoil the punchline a bit, these will turn out to be the same as the artinian rings defined below.

Definition 5.10. A ring is *artinian* if every descending chain of ideals eventually stabilizes. A module is *artinian* if every descending chain of submodules eventually stabilizes.

Example 5.11. Examples of artinian rings include:

- Any field or finite product of fields. For K a field, there is only one ideal, (0). There are $2^n - 1$ ideals of $\underbrace{K \times \cdots \times K}_{n}$, given by all the possible products of i factors equal to (0) and $n - i$ factors equal to K, with $i \geq 1$.
- $R = K[x]/(x^n)$ is an artinian local ring since there are only finitely many ideals for this ring, namely $(\overline{x}^i)$, where $\overline{x}$ is the coset of x in R and $1 \leq i \leq n$.
- $K[x, y]/(x^2, y^2)$, $K[x, y]/(x^2, xy, y^2)$, and $\mathbb{Z}/(p^n)$ are artinian local rings.

- A finitely generated K-algebra A is artinian iff $\dim_K(A) < \infty$. (proven later)

Examples of artinian modules include:

- any finite dimensional K-vector space is an artinian K-module.

The following considerations allow to construct many more artinian rings and modules. Recall the same properties are true for noetherian modules; see Lemma 1.56 and related results.

Lemma 5.12. *1. If R is an artinian ring, then R/I is an artinian ring for any ideal I of R.*

2. If $0 \to N \to M \to L \to 0$ is an exact sequence of R-modules then M is artinian if and only if N and $L = M/N$ are artinian

3. If R is an artinian ring then R^n is an artinian module for all $n \geq 1$.

4. if R is an artinian ring and M is a finitely generated R-module then M is an artinian module.

Exercise 5.13. Prove the above Lemma.

Example 5.14. Looking at our example $R = K[x]/(x^n)$ from above more closely, and in particular at its longest descending chain of ideals

$$(0 = \overline{x}^n) \subseteq (\overline{x}^{n-1}) \subseteq \cdots \subseteq (\overline{x})$$

notice that the successive quotients are fields: $(\overline{x}^{i-1})/(\overline{x}^i) = \overline{x}^{i-1}R/(\overline{x}) \cong R/(\overline{x}) \cong K$.

We now define a class of modules that satisfies a similar property.

Definition 5.15. A nonzero R-module is *simple* if it has no nonzero proper submodules.

There is a useful alternate characterization:

Lemma 5.16. *M is simple if and only if $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.*

Proof. The nontrivial implication comes from the fact that any nonzero module contains a cyclic module, and if $M \cong R/I$ with I not maximal, we can surject to $R/\mathfrak{m}$ for a maximal ideal containing I, which has a proper kernel. □

Definition 5.17. A module M has *finite length* if it has a filtration of the form

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

with M_{i+1}/M_i simple for each i; such a filtration is called a *composition series* of *length* n. Two composition series are *equivalent* if the collections of composition factors M_{i+1}/M_i are the same up to reordering.

The *length* of a finite length module M, denoted $\ell(M)$, is the minimum of the lengths of a composition series of M.

Example 5.18. Any finite dimensional K-vector space V is a finite length module of length $\ell(V) = \dim_K(V)$. So from this perspective one can think of length as a generalization of the notion of vector space dimension.

More generally, we have:

Corollary 5.19. *If $(R, \mathfrak{m}, k)$ is local, M is a finite length R-module if and only if M is a finite dimensional k-vector space and $\ell(M) = \dim_k(M)$.*

Proof. By the Lemma 5.16 any simple module is isomorphic to the residue field k and thus any composition series has quotients $M_{i+1}/M_i \cong k$. By the additivity of vector space dimension along short exact sequences we see that the length of any composition series is equal to $\dim_k(M)$. □

At this point, we would like to know if we can use any composition series to compute the length of a module. The answer is yes! This is the contents of the Jordan-Hölder theorem, which was originally developed in group theory.

Theorem 5.20 (Jordan-Hölder theorem)**.** *For a module M of finite length*

1. *any filtration can be refined to a composition series,*
2. *any two composition series have the same length,*
3. *any two composition series are equivalent.*

Proof. We prove assertion (2) by first showing

Claim: If $N \subseteq M$, then $\ell(N) \leq \ell(M)$, with equality only if $M = N$.

Indeed consider a composition series for M

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

and set $N_i = N \cap M_i$. Then we have a filtration for N

$$0 = N_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

and N_{i-1}/N_i is a submodule of the simple module M_{i-1}/M_i, so either $N_{i-1}/N_i = 0$ or $N_{i-1}/N_i = M_{i-1}/M_i$. Removing N_i from the filtration whenever the former case occurs gives a composition series for N, hence $\ell(N) \leq \ell(M)$ and equality occurs iff $M_i = N_i$ for all i, in particular $M = N$.

Applying the Claim to any composition series of M as above gives

$$\ell(M) > \ell(M_{n-1}) > \cdots > \ell(M_2) > \ell(M_1) > \ell(M_0) = 0,$$

thus $\ell(M) \geq n$. But $\ell(M)$ is defined as the smallest length of a composition series, so we must have $\ell(M) = n$. □

Example 5.21. We have seen in Example 5.18 that every finite dimensional vector space is a finite length module. However there are many more finite length modules.

Consider the local ring $(R = K[x,y]_{(x,y)}, \mathfrak{m} = (x,y))$. Then $M = R/\mathfrak{m}^2$ has length 3, since we have a composition series $0 \subseteq xM \subseteq (x,y)M \subseteq M$; note that each factor is a copy of $R/\mathfrak{m}$. However, M is not an $R/\mathfrak{m}$-vector space since M is not annihilated by $\mathfrak{m}$.

April 7, 2021

Corollary 5.22. *A finite length module M is both an artinian and a noetherian module.*

Proof. This is because a descenending chain of submodules

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

gives rise to inequalities between lengths $\ell(M_0) \geq \ell(M_1) \geq \ell(M_2) \geq \cdots \geq 0$ by the Claim in the previous theorem. Because all these lengths are bounded above by $\ell(M)$ only finitely many of these inequalities can be strict and hence by the Claim in the previous theorem only finitely many of the containments $M_i \supseteq M_{i+1}$ can be strict. If follows that the chain stabilizes.

A similar proofs works for descending chains. □

Even though we will see in Theorem 5.26 that every artinian ring is noetherian and finite length, **it is not true that artinian modules are always noetherian or finite length.**

Exercise 5.23. Fix a prime integer p and let $M = \mathbb{Z}[1/p]/\mathbb{Z}$ viewed as a $\mathbb{Z}$-module. Prove that M is an artinian module, but not a noetherian module and not a finite length module.

Hint: Show that any submodule N of M either contains $1/p^n$ for all n, or else there is a largest n for which $1/p^n \in N$, $N = (\mathbb{Z} \cdot 1/p^n)/\mathbb{Z}$, and this module has finite length.

We next give a characterization of artinian rings as modules of finite length over themselves. We will also see that artinian rings have a finite and discrete spectrum.

To get started on that, we will give a result on primary decomposition for certain ideals in not necessarily noetherian rings.

Proposition 5.24. *Let R be a ring, not necessarily noetherian. Let I be an ideal such that $V(I)$ is a finite set of maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Then, there is a primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t = \mathfrak{q}_1 \cdots \mathfrak{q}_t$ and $R/I \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_t$.*

Proof. First, we claim that $IR_{\mathfrak{m}_i}$ is $\mathfrak{m}_i R_{\mathfrak{m}_i}$-primary. Indeed, note that $V(IR_{\mathfrak{m}_i}) = \{\mathfrak{m}_i R_{\mathfrak{m}_i}\}$ and thus by a homework problem we have $\sqrt{IR_{\mathfrak{m}_i}} = \cap_{\mathfrak{p} \in V(IR_{\mathfrak{m}_i})} \mathfrak{p} = \mathfrak{m}_i R_{\mathfrak{m}_i}$. Thus, if $x, y \in R_{\mathfrak{m}_i}$ are such that $xy \in IR_{\mathfrak{m}_i}$, then either $y^n \in IR_{\mathfrak{m}_i}$ for some $n \in \mathbb{N}$ or and $y \notin \sqrt{IR_{\mathfrak{m}_i}} = \mathfrak{m}_i R_{\mathfrak{m}_i}$. In the latter case, y is a unit in the local ring $R_{\mathfrak{m}_i}$, so $x = xyy^{-1} \in IR_{\mathfrak{m}_i}$. This establishes the claim.

For each i set $\mathfrak{q}_i = IR_{\mathfrak{m}_i} \cap R$. We know that the contraction of a primary ideal is primary so $\mathfrak{q}_i$ is $\mathfrak{m}_i$-primary, and we also know that $I \subseteq \mathfrak{q}_i$ for each i, so $I \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$. We want to show the equality $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ holds. For this, it suffices to check the equality locally at every maximal ideal of R, i.e. we use that for ideals $I \subseteq J$ we have $I = J$ if and only if $IR_{\mathfrak{m}} = JR_{\mathfrak{m}}$ for each $\mathfrak{m} \in \mathrm{mSpec}(R)$.

If $\mathfrak{m} \in \mathrm{mSpec}(R) \setminus V(I)$, then $IR_{\mathfrak{m}} = (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t)R_{\mathfrak{m}} = R_{\mathfrak{m}}$, otherwise,

$$(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t)R_{\mathfrak{m}_i} = q_i R_{\mathfrak{m}_i} = (IR_{\mathfrak{m}_i} \cap R)R_{\mathfrak{m}_i} = IR_{\mathfrak{m}_i}$$

since $\mathfrak{q}_j \not\subseteq \mathfrak{m}_i$ for $j \neq i$. Thus, we have the desired primary decomposition.

The fact that this intersection is a product and the quotient ring is a direct product follows from the Chinese remainder theorem as soon as we establish that $\mathfrak{q}_i + \mathfrak{q}_j = R$, i.e. each pair of ideals is comaximal. Suppose not, then there is some maximal ideal $\mathfrak{m}$ such that $\mathfrak{q}_i + \mathfrak{q}_j \subseteq \mathfrak{m}$. But this implies $\mathfrak{q}_i \subseteq \mathfrak{m}$ and $\mathfrak{q}_j \subseteq \mathfrak{m}$ and by taking radicals $\mathfrak{q}_i \subseteq \mathfrak{m}$ and $\mathfrak{m}_j \subseteq \mathfrak{m}$. By maximality of $\mathfrak{m}_i, \mathfrak{m}_j$ we now have $\mathfrak{m}_i = \mathfrak{m} = \mathfrak{m}_j$, a contradiction.

□

April 9, 2021

We will also need the following lemma:

Lemma 5.25. *If a finitely generated ideal I is generated by nilpotent elements, then there exists $n \geq 1$ so that $I^n = (0)$.*

Proof. Suppose $I = (f_1, \ldots, f_s)$ and $f_i^{n_i} = 0$ for some $n_i \in \mathbb{N}$. Then, using the definition of the powers of I and the pigeonhole principle one sees that

$$I^{\sum_{i=1}^{s}(n_i - 1)+1} = (0).$$

□

We now come to the promised statement about artinian rings.

Theorem 5.26. *The following are equivalent:*

1. *R is noetherian of dimension zero.*
2. *R is a finite product of local noetherian rings of dimension zero.*
3. *R has finite length as an R-module.*
4. *R is artinian.*

When these hold, $\mathrm{Spec}(R)$ *is a finite set and the Zariski topology on this set is the discrete topology.*

Proof. (1)⇒(2): Since R is noetherian of dimension zero, every prime is both maximal and minimal in the poset $\mathrm{Spec}(R)$. Write a minimal primary decomposition for the 0 ideal as

$$0 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$$

with $\mathfrak{q}_i$ being $\mathfrak{m}_i$-primary for some (necessarily maximal) ideals $\mathfrak{m}_i$ such that $\mathfrak{m}_i \neq \mathfrak{m}_j$ for $i \neq j$. As in the proof of Proposition 5.24 $\mathfrak{q}_i + \mathfrak{q}_j = R$ whenever $i \neq j$. By the Chinese remainder theorem we now have

$$R = R/(0) = R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_t.$$

Each factor in this product is a noetherian local ring (with maximal ideal $\mathfrak{m}_i/\mathfrak{q}_i$) of dimension zero.

(2)⇒(3): It suffices to deal with the case $(R, \mathfrak{m})$ is local and of dimension zero. In this case, the maximal ideal is the unique element of $V((0))$, so we have $\sqrt{(0)} = \mathfrak{m}$. Since R is noetherian, $\mathfrak{m}$ is finitely generated, so Lemma 5.25 yields $\mathfrak{m}^n = 0$ for some n. If $\mathfrak{m} = (f_1, \ldots, f_t)$, with t finite since R is noetherian, each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is generated by $\{f_1^{a_1} \cdots f_t^{a_t} \mid a_1 + \cdots + a_t = i\}$ as a $(R/\mathfrak{m})$-vector space, hence has finite length, so the total length of R is finite.

(3)⇒(4): We have obsered this above in Lemma 5.22.

(4)⇒(1): First we show that R has dimension zero. If $\mathfrak{p}$ is any prime, then $A = R/\mathfrak{p}$ is artinian since the ideals of $R/\mathfrak{p}$ are in bijection with a subset of the ideals of R. Pick $a \in A$ some nonzero element. The ideals

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$$

stabilize, so $a^n = a^{n+1}b$ for some b. Since A is a domain, $ab = 1$ in A, so a is a unit. Thus, $R/\mathfrak{p}$ is a field, so every prime is maximal.

Second, note that there are only finitely many maximal ideals. Otherwise, consider the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots.$$

This stabilizes, so $\mathfrak{m}_{n+1} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$. By distinctness, we can pick $f_i \in \mathfrak{m}_i \smallsetminus \mathfrak{m}_{n+1}$, but then $f_1 \cdots f_n \in \mathfrak{m}_1 \cdots \mathfrak{m}_n \smallsetminus \mathfrak{m}_{n+1}$, which is a contradiction. Now, we apply Proposition 5.24 to conclude that R is a finite direct product of local rings of dimension zero. Since each of the factors is a quotient ring, each is artinian. It suffices to show that each factor is noetherian, so WLOG assume that $(R, \mathfrak{m})$ is local.

Now, to see R is noetherian, $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$ stabilizes again, so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$; we can't apply NAK yet since we don't know $\mathfrak{m}^n$ is finitely generated. If $\mathfrak{m}^n \neq 0$, consider the family S of ideals $I \subseteq \mathfrak{m}$ such that $I\mathfrak{m}^n \neq 0$; this contains $\mathfrak{m}$. Just as the noetherian property guarantees maximal elements of nonempty families, the artinian property guarantees minimal elements; take J minimal in S. For some $x \in J$, $x\mathfrak{m}^n \neq 0$, and $(x) \subseteq J \subseteq \mathfrak{m}$, so $J = (x)$ is principal by minimality. Now, $x\mathfrak{m}(\mathfrak{m}^n) = x\mathfrak{m}^{n+1} = x\mathfrak{m}^n \neq 0$, so $x\mathfrak{m} \subseteq (x)$ is in the family S of ideals, and by minimality, $(x) = \mathfrak{m}(x)$. NAK applies to this, so $(x) = (0)$, contradicting that $\mathfrak{m}^n \neq 0$. Then, we have

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m} \subseteq R,$$

and since the artinian property descends to submodules and quotients, each factor has finite length. Thus, R has finite length, R is noetherian by Lemma 5.22, as desired.

The fact that the spectrum is finite has been proven in (4). The fact that the Zariski topology on $\mathrm{Spec}(R)$ is the discrete topology follows because in a zero dimensional ring all prime ideals are maximal, thus each of the singleton subsets of $\mathrm{Spec}(R)$ is closed. □

Another useful characterization of artinian local rings is given below:

Proposition 5.27. *For a noetherian local ring $(R, \mathfrak{m})$ the following are equivalent:*

1. *$(R, \mathfrak{m})$ is a local artinian ring*
2. *$\mathfrak{m}^N = 0$ for some $N \geq 1$, i.e. the ideal $\mathfrak{m}$ is nilpotent.*

Proof. (1) $\Rightarrow$ (2) The powers of $\mathfrak{m}$ form a descending chain, so they stabilize, i.e. $\mathfrak{m}^N = \mathfrak{m}^{N+1}$ for some $N \in \mathbb{N}$. Since R is artinian it is noetherian too by Theorem 5.26, so NAK implies that $\mathfrak{m}^N = 0$.

(2) $\Rightarrow$ (1) The ideals $0 = \mathfrak{m}^N \subseteq \mathfrak{m}^{N-1} \subseteq \cdots \subseteq \mathfrak{m}^2 \subseteq \mathfrak{m} \subseteq R$ form a filtration of R, with finite length quotients as in the proof of (2) $\Rightarrow$ (3) of Theorem 5.26, hence R is finite length as a module over itself by Lemma 5.22 (2) and consequently an artinian ring by Theorem 5.26. □

April 13, 2020

5.3 The Hilbert function of a graded algebra

A useful bit of extra structure that one commonly encounters, and that we have already used even, is that of a grading on a ring.

Definition 5.28. Let R be a ring, and T be a monoid. The ring R is *T-graded* if there exists a direct sum decomposition of R as an abelian group indexed by T: $R = \bigoplus_{a \in T} R_a$ such that, for any $a, b \in T$, and any $r \in R_a, s \in R_b$, one has $rs \in R_{a+b}$. An element that lies in one of the summands R_a is said to be *homogeneous* of *degree* a.; we often use $|r|$ to denote the degree of a homogeneous element r.

We can also talk about graded modules.

Definition 5.29. Let R be a ring, M an R-module and $(T, +)$ a monoid. M is *T-graded* if there exists a direct sum decomposition of M as an abelian group indexed by T: $M = \bigoplus_{a \in T} M_a$ such that, for any $a, b \in T$, and any $r \in R_a, s \in M_b$, one has $rs \in M_{a+b}$. An element that lies in one of the summands M_a is said to be *homogeneous* of *degree* a.

Example 5.30. The most common instances of graded rings are $\mathbb{N}$-graded $R = \bigoplus_{d \geq 0} R_d$ or $\mathbb{Z}$-graded $R = \bigoplus_{d \in \mathbb{Z}} R_d$.

Remark 5.31. By definition, an element in a graded ring or module is, in a unique way, a sum of homogeneous elements, which we call its *homogeneous components* or graded components. In other words, $\sum_{t\in T} f_t = \sum_{t\in T} g_t$ where $f_t, g_t \in R_t$ if and only if $f_t = g_t$ for each $t \in T$. This is often used in practice to reduce to proving statements about homogeneous polynomials.

Remark 5.32. Let 0 be the identity element of the monoid T. If R is a T-graded ring then for any $t \in T$, $r \in R_0, s \in R_t$, one has $rs \in R_t$ so R_t is a R_0-module and R_0 is a subring of R.

If M is a T-graded R-module then similarly for all $t \in T$ M_t is an R_0-module.

Definition 5.33. An $\mathbb{N}$-graded ring R is *standard graded* if R is generated as an R_0-algebra by R_1.

Example 5.34.

1. If K is a field, and $R = K[x_1, \ldots, x_n]$ is a polynomial ring, then there is an $\mathbb{N}$-grading on R where R_d is the K-vector space with basis given by monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\sum_{i=1}^n \alpha_i = d$. Of course, this is the notion of degree familiar from Math 818 and before. This is called the *standard grading*.

2. With K is a field, and $R = K[x_1, \ldots, x_n]$ as above, for any $(\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, one can give a different $\mathbb{N}$-grading on R by letting x_i have degree β_i for some integers β_i; we call this a grading with *weights* $(\beta_1, \ldots, \beta_n)$.

   For example, in $K[x_1, x_2]$, $x_1^2 + x_2^3$ is not homogeneous in the standard grading, but is homogeneous of degree 6 under the $\mathbb{N}$-grading with weights $(3, 2)$.

3. Again with K and R as above, R admits an $\mathbb{N}^n$-grading, with $R_{(d_1,\ldots,d_n)} = K \cdot x_1^{d_1} \cdots x_n^{d_n}$. This is called the *fine grading*.

Definition 5.35. An ideal I in a graded ring R is called *homogeneous* if it can be generated by homogeneous elements.

We now observe the following:

Lemma 5.36. *Let R be an T-graded ring, and I be a homogeneous ideal. Then $R/I = \bigoplus_{t\in T} R_t/I_t$ is also T-graded.*

Exercise 5.37. Prove the above Lemma.

Definition 5.38. Let R and S be T-graded rings (same grading monoid). A ring homomorphism $\varphi : R \to S$ is *degree-preserving* if $\varphi(R_a) \subseteq S_a$ for all $a \in T$.

Remark 5.39. The class of graded rings and degree-preserving functions forms a category $\langle\langle$Gr. Rings$\rangle\rangle$. In the same way as the category of reduced K-algebras is equivalent to that of affine algebraic sets, the category of reduced standard graded K-algebras is equivalent to that of projective algebraic sets, which are algebraic subsets of the projective space $\mathbb{P}^n_K$.

We now introduce a generating function (a useful combinatorial book keeping tool) for the vector space dimensions of the graded components of a finitely generated K-algebra.

Definition 5.40. If R is an T-graded ring, the *Hilbert function* of R is the function $h_R : \mathbb{N} \mapsto \mathbb{N} \cup \{\infty\}$ with values $h_R(t) := \ell_{R_0}(R_t)$. Here $\ell(R_t)$ denotes the length of R_t is an R_0-module.

Similarly, if M is an $\mathbb{N}$-graded R-module, we define the Hilbert function of M by $h_M : \mathbb{N} \mapsto \mathbb{N} \cup \{\infty\}, h_M(t) = \ell_{R_0}(M_t)$.

If $T = \mathbb{N}$, we define the *Hilbert series* of R or of an R-module M as above by $H_R(z) = \sum_{i\in\mathbb{N}} h_R(i)z^i$ and $H_M(z) = \sum_{i\in\mathbb{N}} h_M(i)z^i$.

(The textbook calls this Poicaré series, but in modern terminology that means something else.)

Example 5.41. Consider the standard graded ring

$$R = K[x,y]/(x^2,y^3) = \underbrace{K}_{R_0} \bigoplus \underbrace{(Kx \oplus Ky)}_{R_1} \bigoplus \underbrace{(Kxy \oplus Ky^2)}_{R_2} \bigoplus \underbrace{Kxy^2}_{R_3}.$$

Then $h_R(t) = \begin{cases} 1 & \text{if } t = 0 \\ 2 & \text{if } t = 1,2 \\ 1 & \text{if } t = 3 \\ 0 & \text{if } t \geq 4 \end{cases}$ and $H_R(z) = 1 + 2z + 2z^2 + z^3$. Notice that $h_R(t)$ is eventually the zero function, which we will take by convention to have degree -1 as a polynomial. Note also that $\dim(R) = 0$ since R is a finite dimensional K-algebra (finite length), hence an artinian ring.

April 14, 2021

The key example of a Hilbert function is that of a polynomial ring.

Example 5.42. Let K be a field, and $R = K[x_1,\ldots,x_n]$ be a polynomial ring with the standard grading: $|x_i| = 1$ for each i. To compute the Hilbert function, we need to compute the size of a K-basis for $H_R(t)$ for each t. We have

$$R_t = \bigoplus_{a_1+\cdots+a_n=t} Kx_1^{a_1}\cdots x_n^{a_n}.$$

We can find a bijection between these monomials and the set of strings that contain t stars and $n-1$ bars, where the monomial $x_1^{a_1}\cdots x_n^{a_n}$ corresponds to the string with a_1 stars, then a bar, then a_2 stars, a bar, etc. Thus, the number of monomials is the number of ways to choose $n-1$ bars from $t+n-1$ spots, i.e.,

$$h_R(t) = \binom{t+n-1}{n-1} \quad \text{for } t \geq 0.$$

We observe the binomial function here can be expressed as a polynomial in t for $t \geq 0$; let

$$P_n(t) = \frac{(t+n-1)(t+n-2)\cdots(t+1)}{(n-1)!} \in \mathbb{Q}[t].$$

Observe that $P_n(t)$ has $-1, \ldots, -(n-1)$ as roots. Then we have

$$h_R(t) = \begin{cases} P_n(t) & \text{if } t > -n \\ 0 & \text{if } t < 0. \end{cases}$$

Note that the two cases overlap for $t = -(n-1), \ldots, -1$.

Notice that in this example the Hilbert function is eventually (for $t \geq -n$) equal to a polynomial of degree $n-1$. Moreover recall that $\dim(R) = n$.

To compute the Hilbert series, notice that the number of monomials of degree d is equal to the number of ordered tuples $(a_1, \ldots, a_n)$ with $\sum_{i=1}^n = d$. This is the coefficient of z^d in the product

$$(1+z+z^2+\cdots+z^{a_1}+\cdots)(1+z+z^2+\cdots+z^{a_2}+\cdots)\cdots(1+z+z^2+\cdots+z^{a_n}+\cdots)$$

hence

$$H_R(z) = (1+z+z^2+\cdots+z^i+\cdots)^n = \frac{1}{(1-z)^n}.$$

A very important property of length that makes the theory of Hilbert functions work is its additivity on short exact sequences:

Lemma 5.43. *If L, M, N are R-modules that form a short exact sequence $0 \to L \to M \to N \to 0$ then M has finite length if and only if L and N have finite lengths and in this case there is an equality $\ell(M) = \ell(L) + \ell(N)$.*

We can generalize Example 5.42 as follows.

Theorem 5.44 (Hilbert-Serre)**.** *Let R_0 be an artinian ring and let $R = R_0[x_1, \ldots, x_n]$ be a finitely generated R_0-algebra graded by $|x_i| = d_i$. The Hilbert series $H_M(z)$ of any finitely generated R- module M is a rational function of the form*

$$H_M(z) = \frac{f(z)}{\prod_{i=1}^n (1-z^{d_i})} \text{ with } f \in \mathbb{Z}[z]$$

Proof. By induction on n.

If $n = 0$ then $R = R_0$ and M is a finitely generated R_0-module. Since R_0 is an artinian ring $\ell(R_0) < \infty$ by Theorem 5.26. Since M is a finitely generated R_0-module, it is a quotient of R_0^m for some $m \geq 0$. Thus $\ell(M) \leq \ell(R_0^m) = m\ell(R_0) < \infty$ by Lemma 5.43. This yields that $\ell(M_t) = 0$ for $t \gg 0$ thus $H_M(z) = f(z)$ for some $f \in \mathbb{N}[z]$. (In this case the Hilbert series is a polynomial.)

For the induction step, multiplication by x_n on M induces an exact sequence

$$0 \to K \to M \xrightarrow{x_n} M \to N \to 0$$

where $K = \{m \in M \mid x_n m = 0\}$ and $N = M/(x_n)M$. Because K and N are annihilated by x_n they are finitely generated modules over $R/(x_n) = R_0[x_1, \ldots, x_{n-1}]$. The exact sequence above decomposes into a direct sum of exact sequences of R_0 modules of the form

$$0 \to K_t \to M_t \xrightarrow{x_n} M_{t+d_n} \to N_{t+d_n} \to 0$$

Additivity of length yields

$$\ell(K_t) - \ell(M_t) + \ell(M_{t+d_n}) - \ell(N_{t+d_n}) = 0$$

or

$$h_K(t) - h_M(t) + h_M(t + d_n) - h_N(t + d_n) = 0.$$

In terms of Hilbert series this gives after multiplying by z^{t+d_n} and summing up

$$z^{d_n} H_K(t) - z^{d_n} H_M(t) + H_M(t + d_n) - H_N(t + d_n) = 0$$

or

$$(1 - z^{d_n}) H_M(t) = H_N(t) - z^{d_n} H_K(t).$$

Applying the inductive hypothesis for $H_N(t)$ and $H_K(t)$ and substituting into the above identity yields the desired conclusion. □

Remark 5.45. When R has the standard grading ($|x_i| = 1$ for all $1 \leq i \leq n$) then the Hilbert series in the Hilbert-Serre theorem becomes

$$H_M(z) = \frac{f(z)}{(1 - z)^n} \text{ with } f \in \mathbb{Z}[z].$$

However this may not be in reduced form. The reduced form will be

$$H_M(z) = \frac{h(z)}{(1 - z)^{d(M)}} \text{ with } h \in \mathbb{Z}[z], h(1) \neq 0 \text{ and } d(M) \geq 0. \tag{5.1}$$

Definition 5.46. For a graded module M over a graded ring R we denote by $d(M)$ the order of the pole of $H_M(z)$ at $z = 1$. This is defined as follows: if $H_M(z) = \frac{f(z)}{g(z)}$ in lowest terms, then

$$d(M) = \max\{n \mid (1 - z)^n \mid g(z)\}.$$

If R is standard graded, this allows to express $H_M(z)$ as in equation (5.1).

Example 5.47. The standard graded polynomial ring $R = K[x_1, \ldots, x_n]$ has $d(R) = n$ according to Example 5.42.

Corollary 5.48. *Let R_0 be an artinian ring and let R be a finitely generated standard graded R_0-algebra. The Hilbert function $h_M(z)$ of any finitely generated R-module M is given for sufficiently large t by a polynomial $P_M(t) \in \mathbb{Q}[t]$ of degree $d(M) - 1$. In particular the degree of $P_M(t)$ is at most the number of generators of R as an R_0-algebra minus 1.*

Proof. Use the formula for the Hilbert series

$$H_M(z) = \frac{h(z)}{(1-z)^{d(M)}} \text{ with } h \in \mathbb{Z}[z]$$

from the Hilbert-Serre theorem, the "negative binomial" formula

$$\frac{1}{(1-z)^{d(M)}} = \sum_{i=0}^{\infty} \binom{i + d(M) - 1}{d(M) - 1} z^i.$$

and the fact that the binomial coefficients above are polynomials in i of degree $d(M)-1$ for $i \gg 0$. □

Definition 5.49. The *Hilbert polynomial* of a standard graded module is the polynomial $P_M(t)$ that agrees with $h_M(t)$ for $t \gg 0$.

Example 5.50. The Hilbert polynomial of a standard graded ring $R = K[x_1, \ldots, x_n]$ is $P_R(t) = \frac{(t+n-1)(t+n-2)\cdots(t+1)}{(n-1)!} \in \mathbb{Q}[t]$ as discussed in Example 5.42.

5.4 Associated graded rings, Hilbert-Samuel function

Graded rings and modules from filtrations

Next I want to introduce a way of constructing graded rings and modules from ungraded ones. For this we need to define a special type of filtration.

Definition 5.51. Let R be a ring, I an ideal and M an R-module. A filtration of M is a possibly infinite descending chain of submodules

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq M_{n+1} \cdots$$

The filtration is and *I-filtration* if $IM_n \subseteq M_{n+1}$ for all $n \in \mathbb{N}$ and it is *I-stable* if $IM_n = M_{n+1}$ for all $n \gg 0$.

Example 5.52. Setting $M_n = I^n M$ gives a stable I-filtration. In particular, for $M = R$ this filtration is

$$R = I^0 \supseteq I \supseteq I^2 \cdots \supseteq I^n \supseteq I^{n+1} \cdots$$

Definition 5.53. The *Rees algebra* of I is a standard graded ring obtained from the above filtration by taking its external direct sum as follows

$$\mathcal{R}(I) = \bigoplus_{n\in\mathbb{N}} I^n.$$

An alternative way to define the Rees algebra of I is to describe it as a subring of the graded ring $R[t]$ (where $\deg(t) = 1$) using an internal direct sum:

$$\mathcal{R}(I) = \bigoplus_{n\in\mathbb{N}} I^n t^n = \{a_0 + a_1 t + a_2 t^2 + \cdots + a_m t^m \in R[t] \mid a_i \in I^i \forall i\}.$$

Then $\mathcal{R}(I)$ is a graded subring of $R[t]$. The advantage to this approach is that the exponent of the variable t identifies the degrees of the homogeneous components of a particular element of $\mathcal{R}(I)$.

Exercise 5.54. Let R be a ring and $I = (f_1, \ldots, f_k)$ a finitely generated ideal. Prove that $\mathcal{R}(I) = R[f_1 t, \ldots, f_k t]$. In particular, this shows that $\mathcal{R}(I)$ is a finitely generated R-algebra. If R is noetherian this indicates that $\mathcal{R}(I)$ is a finitely generated R-algebra for any ideal I.

Definition 5.55. Let R be a ring, I an ideal and M an R-module equipped with an I-filtration $\mathcal{F} = \{M_n\}_{n\in\mathbb{N}}$. This filtration gives rise to the graded module

$$\mathcal{R}(\mathcal{F}) = \bigoplus_{n\in\mathbb{N}} M_n.$$

This module $\mathcal{R}(\mathcal{F})$ is a $\mathcal{R}[I]$-module. The multiplication goes as expected : if $a \in I^n$ and $m \in M_{n'}$ then their product is

$$am \in I^n M_{n'} \subseteq M_{n+n'}.$$

The definition of graded module is satisfied since $I_n M'_n \subseteq M_{n+n'}$ for all $n, n' \in \mathbb{N}$ which is a consequence of the definition for I-filtration.

April 19, 2021

Theorem 5.56. *Let R be a Noetherian ring, I an ideal and M a finitely generated R-module equipped with an I-filtration $\mathcal{F} = \{M_n\}_{n\in\mathbb{N}}$. The following are equivalent:*

1. *the filtration is I-stable*
2. *$\mathcal{R}(\mathcal{F})$ is a finitely generated $\mathcal{R}(I)$-module.*

Proof. By Exercise 5.54 and Hilbert's basis theorem, $\mathcal{R}(I)$ is a noetherian ring.

Since M is finitely generated and R is Noetherian, each submodule M_n is finitely generated. Consequently each finite direct sum $Q_n := \bigoplus_{i=0}^{n} M_i$ is finitely generated is finitely generated as an R-module. Then the $\mathcal{R}(I)$-submodule of $\mathrm{gr}_{\mathcal{F}}(M)$ generated by Q_n, denoted $Q_n\mathcal{R}(I)$, is a finitely generated $\mathcal{R}(I)$-module (same generators).

Now there is a ascending chain of $\mathcal{R}(I)$-modules

$$\cdots \subseteq Q_n\mathcal{R}(I) \subseteq Q_{n+1}\mathcal{R}(I) \subseteq \cdots$$

whose union is $\mathrm{gr}_{\mathcal{F}}(M)$. Then $\mathrm{gr}_{\mathcal{F}}(M)$ is a finitely generated $\mathcal{R}(I)$-module if and only if the chain stabilizes. Looking more closely at Q_n we see that

$$Q_n\mathcal{R}(I) = \bigoplus_{i=0}^{n} M_i \oplus IM_n \oplus I^2M_n \oplus \cdots$$

Thus the chain stabilizes iff $M_{n+i} = I^iM_n$ for all $n \gg 0$, that is, the filtration $\mathcal{F}$ is a-stable. □

Now we come to an important theorem about I-stable filtrations:

Theorem 5.57 (Artin-Rees)**.** *Let R be a Noetherian ring, I an ideal of R. If N is a submodule of M and $\mathcal{F} = \{M_n\}_{n\in\mathbb{N}}$ is an I-stable filtration on M then setting $N_n = M_n \cap N$ gives an I-stable filtration $\mathcal{F}' = \{N_n\}_{n\in\mathbb{N}}$ of N.*

In particular, there exists $k \in \mathbb{N}$ such that

$$I^nM \cap N = I^{n-k}(I^kM \cap N) \text{ for } n \geq k.$$

Proof. The fact that $\mathcal{F}'$ is a filtration follows from its definition. By Theorem 5.56 $\mathcal{R}(\mathcal{F})$ is a finitely generated $\mathcal{R}(I)$-module and $\mathcal{R}(I)$ is Noetherian. Moreover $\mathcal{R}(\mathcal{F}')$ is a submodule of $\mathcal{R}(\mathcal{F})$. Since the latter is finitely generated so is $\mathcal{R}(\mathcal{F}')$). By Theorem 5.56, $\mathcal{F}'$ is thus I-stable.

To see the "in particular" set $M_n = I^nM$ and notice that the displayed equality is the definition for the resulting filtration $N_n = I^nM \cap N$ to be I-stable. □

Associated graded rings

We next wish to construct different graded rings from the previously mentioned filtrations which bear the name associated graded rings.

Definition 5.58. The *associated graded ring* of an ideal I in a ring R is the ring

$$\mathrm{gr}_I(R) := \bigoplus_{n\in\mathbb{N}} \frac{I^n}{I^{n+1}} = \frac{\mathcal{R}(I)}{I\mathcal{R}(I)},$$

with n-th graded piece I^n/I^{n+1}, and multiplication

$$(a + I^{n+1})(b + I^{m+1}) = ab + I^{m+n+1} \text{ for } a \in I^n, b \in I^m.$$

If $(R, \mathfrak{m})$ is local, then $\mathrm{gr}(R) := \mathrm{gr}_{\mathfrak{m}}(R)$ will be called the associated graded ring of R.

Remark 5.59. Note that the multiplication is well-defined. Indeed if $a \in I^n, b \in I^m, u \in I^{n+1}, v \in I^{m+1}$, that is, $a + u \in a + I^{n+1}$ and $b + v \in b + I^{m+1}$ then

$$(a + u)(b + v) = ab = av + bu + uv \in ab + I^{m+n+1}.$$

Remark 5.60. We observe also from the definitions that

- $\mathrm{gr}_I(R)$ is a standard graded ring because it is a quotient of the standard graded ring $\mathcal{R}(I)$
- $[\mathrm{gr}_I(R)]_0 = R/I$; if $(R, \mathfrak{m}, k)$ is local then $[\mathrm{gr}(R)]_0 = R/\mathfrak{m} = k$
- each graded piece $[\mathrm{gr}(R)]_n = I^n/I^{n+1}$ is an R-module annihilated by I, so it is an R/I-module. If $(R, \mathfrak{m}, k)$ is local then $[\mathrm{gr}(R)]_n$ is a k-vector space.

Remark 5.61. There is a surjective map $^* : R \to \mathrm{gr}_I(R)$ given by $f \mapsto f^*$ where f^* is the image of f in I^v/I^{v+1} for $v = \min\{i \mid f \in I^i\}$. **This map is not a ring homomorphism.** When R is local and $I = \mathfrak{m}$, f^* has a nice interpretation as the term(s) of lowest degree of f.

This map helps in finding the associated graded ring of a quotient as follows:

$$\mathrm{gr}(R/J) = \frac{\mathrm{gr}(R)}{(f^* \mid f \in J)}.$$

April 21, 2021

Example 5.62. Let $R = K[x, y]/(y^2 - x^2(x+1))_{(x,y)}$. This is a local ring with maximal ideal $\mathfrak{m} = (x, y)$. Note that the element $y^2 - x^2(x+1)$ has valuation $v = 2$ with respect to the $\mathfrak{m}$-adic filtration on $k[x, y]$ and that

$$f^* = y^2 - x^2(x + 1) + \mathfrak{m}^3 = y^2 - x^2 + \mathfrak{m}^3.$$

We will compute $\mathrm{gr}(R)$. According to the remark above, we have

$$\mathrm{gr}_{\mathfrak{m}}(R) = \frac{K[x, y]}{(f^* \mid f \in (y^2 - x^2(x + 1))} = \frac{K[x, y]}{(y^2 - x^2)}.$$

Let's see why $y^2 - x^2 = 0$ in $\mathrm{gr}(R)$: this is because in R we have $y^2 - x^2 = x^3 \in \mathfrak{m}^3$, that is the image of $y^2 - x^2$ in $\mathfrak{m}^2/\mathfrak{m}^3$ through the map in Remark 5.61 is 0.

Geometrically, if R is the coordinate ring ov an algebraic set X, then the ring $\mathrm{gr}_{\mathfrak{m}}(R)$ is the coordinate ring of the tangent cone to X at the origin. In this example we see that $V(x^2 - y^2)$ is the union of two lines $V(x - y)$ and $V(x + y)$ which are the two tangent lines to the nodal cubic at the point $(0, 0)$.

Hilbert-Samuel functions

Definition 5.63. For $(R, \mathfrak{m})$ local, we set $H_R(t) = H_{\mathrm{gr}(R)}(t)$ and $h_R(t) = h_{\mathrm{gr}(R)}(t)$. We call this the *Hilbert function* and *Hilbert series* of the local ring R.

Definition 5.64. For an ideal I of a ring R so that R/I is artinian we define the *Hilbert-Samuel function* of R with respect to I to be $\chi_I^R(n) = \ell_{R/I}(R/I^n)$.

Remark 5.65. We have a filtration of R/I^n as follows

$$R/I^n \subseteq I/I^n \subseteq I^2/I^n \subseteq \cdots \subseteq I^{n-1}/I^n \subseteq 0$$

with quotients $(I^i/I^n)/(I^{i+1}/I^n) \cong I^i/I^{i+1}$. Since length is additive along filtrations it follows that

$$\chi_I^R(n) = \ell_{R/I}(R/I^n) = \sum_{i=0}^{n-1} \ell_{R/I}(I^i/I^{i+1}) = \sum_{i=0}^{n-1} h_{\mathrm{gr}_I(R)}(i) \tag{5.2}$$

Because of the previous summation formula, we can think of the function χ_I^R as a discrete "integral" of the Hilbert function of $h_{\mathrm{gr}_I(R)}$. Thus if $h_{\mathrm{gr}_I(R)}$ is a polynomial of degree $d-1$ then χ_I^R is a polynomial of degree d.

We now see that under appropriate circumstances Hilbert-Samuel functions, just like Hilbert functions, are eventually given by polynomials.

Theorem 5.66. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal generated by s elements. Then*

1. *the function $h_{\mathrm{gr}_\mathfrak{q}(R)} : \mathbb{N} \to \mathbb{N}$ is eventually (for large enough inputs) equal to a polynomial $P_{\mathrm{gr}_\mathfrak{q}(R)}$ of degree at most $s-1$*
2. *the function $\chi_\mathfrak{q}(R) : \mathbb{N} \to \mathbb{N}$ is eventually (for large enough inputs) equal to a polynomial $g_\mathfrak{q}(R)$ of degree at most s*
3. *$\deg(g_\mathfrak{q}(R)) = \deg(g_\mathfrak{m}(R))$; in particular $\deg(g_\mathfrak{q}(R))$ does not depend on $\mathfrak{q}$, but only on R.*

Proof. Since $\sqrt{\mathfrak{q}} = \mathfrak{m}$ we see that $\mathbb{V}(\mathfrak{q}) = \mathbb{V}(\mathfrak{m}) = \{m\}$ and thus $\dim(R/\mathfrak{q}) = 0$. Since $R/\mathfrak{q}$ is a noetherian ring of Krull dimension 0 it is artinian and therefore has finite length.

(1.) Let $\mathfrak{q} = (f_1, \ldots, f_s)$. Recall that $\mathrm{gr}_\mathfrak{q}(R)$ is a standard graded algebra and it is finitely generated by $f_1^*, \ldots, f_s^*$ as a $R/\mathfrak{q}$-algebra. By Corollary 5.48 the hilbert function of $\mathrm{gr}_\mathfrak{q}(R)$ is eventually equal to its Hilbert polynomial which has degree at most $s-1$.

(2.) Based on part (1.) equation (5.2) and Remark 5.65 show that $\chi_\mathfrak{q}(n)$ is equal to a polynomial $g(n)$ for $n \gg 0$. Furthermore, we have

$$\deg(g) = \deg(P_{\mathrm{gr}_\mathfrak{q}(R)}) + 1 \leq s - 1 + 1 = s.$$

(3.) Suppose that $\mathfrak{m} = (g_1, \ldots, g_t)$. Since $\mathfrak{m} = \sqrt{\mathfrak{q}}$ there exist positive integers n_i such that $g_i^{n_i} \in \mathfrak{q}$ for $1 \leq i \leq t$. Setting $N = \sum_{i=1}^{t}(n_i - 1) - 1$ we see by a pigeonhole argument that $\mathfrak{m}^N \subseteq \mathfrak{q}$. Because $\mathfrak{m}^N \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ we have for each $n \in \mathbb{N}$ that

$$\mathfrak{m}^{nN} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$$

and thus there are inequalities

$$\ell_{R/\mathfrak{m}}(R/\mathfrak{m}^{nN}) = \dim_k(R/\mathfrak{m}^{nN}) \geq \dim_k(R/\mathfrak{q}^n) = \ell_{R/\mathfrak{q}}(R/\mathfrak{q}^n) \geq \ell_{R/\mathfrak{m}}(R/\mathfrak{m}^n) = \dim_k(R/\mathfrak{m}^n)$$

that is

$$\chi^R_{\mathfrak{m}}(Nn) \geq \chi^R_{\mathfrak{q}}(n) \geq \chi^R_{\mathfrak{m}}(n) \text{ or } g_{\mathfrak{m}}(Nn) \geq g_{\mathfrak{q}}(n) \geq g_{\mathfrak{m}}(n) \text{ for } n \gg 0.$$

The last inequality shows that $\deg(g_{\mathfrak{q}}) = \deg(g_{\mathfrak{m}})$. □

Definition 5.67. We call the polynomial $g_{\mathfrak{m}}(R)$ from Theorem 5.66 the *Hilbert-Samuel polynomial* of R.

April 23, 2021

5.5 The dimension theorem

Finally we come to the main theorem regarding the dimension of noetherian local rings.

Theorem 5.68 (The dimension theorem)**.** *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring and consider the numbers*

$$\begin{aligned} dim(R) &= \text{the Krull dimension of } R \\ d(R) &= \text{the degree of the Hilbert-Samuel polynomial of } R \\ \delta(R) &= \text{the smallest number of minimal generators of an } \mathfrak{m}\text{-primary ideal} \end{aligned}$$

Then

$$dim(R) = d(R) = \delta(R).$$

Before we prove this theorem we observe an important consequence.

Corollary 5.69. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. Then* $\dim(R)$ *is finite.*

Proof. This is because $dim(R) = \delta(R) \leq \mu(\mathfrak{m})$ by definition of $\delta(R)$. □

Example 5.70. Let's study again the localization of the coordinate ring of the nodal cubic at $\mathfrak{m}' = (\overline{x}, \overline{y})$

$$R = \left(\frac{K[x,y]}{(y^2 - x^2(x+1))}\right)_{\mathfrak{m}}.$$

This is a local ring $(R, \mathfrak{m}, K)$, where $\mathfrak{m} = \mathfrak{m}'R$.

Since $K[x] \hookrightarrow R$ is a Noether normalization (by definition of R, $\overline{y}$ is integral over $k[\overline{x}]$), we see that $\dim(R) = 1$.

Consider the ideal $\mathfrak{q} = (\overline{x})$ of R and note that since $0 = \overline{y}^2 - \overline{x}^2(\overline{x}+1) \in \mathfrak{q}$ and $\overline{x} \in \mathfrak{q}$ we have $\overline{y}^2 \in \mathfrak{q}$. Thus $\mathfrak{m} = \sqrt{\mathfrak{q}}$ and we deduce that $\mathfrak{q}$ is $\mathfrak{m}$-primary. Hence $\delta(R) \leq 1$ and since 0 is not $\mathfrak{m}$-primary in fact $\delta(R) = 1$.

Finally, we have computed in Example 5.62 the associated graded ring

$$\mathrm{gr}_{\mathfrak{m}}(R) = \frac{K[x,y]}{(y^2 - x^2)} = K \oplus \underbrace{Kx \oplus Ky}_{\deg 1} \oplus \underbrace{Kx^2 \oplus Kxy}_{\deg 2} \oplus \cdots \underbrace{Kx^d \oplus Kx^{d-1}y}_{\deg d} \oplus \cdots .$$

Thus

$$h_{\mathrm{gr}_{\mathfrak{m}}(R)}(d) = \begin{cases} 1 & d = 0 \\ 2 & d \geq 1 \end{cases}$$

and

$$\chi^R_{\mathfrak{m}}(n) = \sum_{d=1}^{n-1} h_{\mathrm{gr}_{\mathfrak{m}}(R)}(d) = 1 + 2(n-2) = 2n - 3.$$

The latter is a polynomial of degree 1 in n so $d(R) = 1$.

For the proof of the Dimension Theorem we will show

$$\delta(R) \geq d(R) \geq \dim(R) \geq \delta(R).$$

Theorem 5.66 shows that $\delta(R) \geq d(R)$. Next we show $\dim(R) \geq \delta(R)$. We will use:

Lemma 5.71 (Prime avoidance)**.** *If $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are ideals in a ring R, with $\mathfrak{p}_i$ prime for each i, and $I \subseteq \bigcup_{i=1}^m \mathfrak{p}_j$, then $I \subseteq \mathfrak{p}_j$ for some j.*

Proof. We prove that if I is not contained in $\mathfrak{p}_j$ for all j then I is not contained in $\bigcup_{j=1}^m \mathfrak{p}_j$ by induction on m. The case $m = 1$ is obvious. For $m > 1$, using the induction hypothesis, we have that for each i there is a $y_i \in I \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. If for some i we have $y_i \notin \mathfrak{q}_i$, we are done. Otherwise, $y_i \in \mathfrak{p}_i$ for all i. Let $\hat{y}_i = y_1 \cdots y_{i-1} y_{i+1} \cdots y_m$.

Note that $\hat{y}_i \notin \mathfrak{q}_i$ for all i, since $y_s \notin \mathfrak{p}_i$ for all $s \neq i$ and $\mathfrak{p}_i$ is prime, and $\hat{y}_i \in \mathfrak{p}_s$ for all $s \neq i$, since we have assumed $y_s \in \mathfrak{p}_s$. Clearly $\hat{y}_i \in I$ for all i. Now set $x = \sum_i \hat{y}_i$. It follows that $x \in I$ and $x \notin \mathfrak{p}_i$ for all i. □

Proposition 5.72. *For a noetherian local ring $(R, \mathfrak{m}, k)$ we have $\dim(R) \geq \delta(R)$.*

Proof. Let $d = \dim(R)$. We will show there is an $\mathfrak{m}$-primary ideal generated by d elements.

We construct by induction on $0 \leq i \leq d$ that there are $x_1, \ldots, x_d \in R$ such that $\mathrm{height}(x_1, \ldots, x_i) \geq i$. The case $i = 0$ gives the 0 ideal which has height 0.

Suppose $i < d$ and $x_1, \ldots, x_i$ have been constructed so that $\mathrm{height}(x_1, \ldots, x_i) \geq i$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the (necessarily minimal) primes in $\mathbb{V}((x_1, \ldots, x_i))$ so that $\mathrm{height}(p_j) = i$, if any such primes exist. Since $\mathrm{height}(\mathfrak{m}) = d > i$ we see that $\mathfrak{m} \neq \mathfrak{p}_j$ for all such

primes. By the prime avoidance Lemma 5.71 we deduce that $\mathfrak{m} \not\subseteq \bigcup_{j=1}^{s} \mathfrak{p}_j$ and so we choose $x_{i+1} \in \mathfrak{m}$ so that $x_{i+1} \notin \mathfrak{p}_j$ for all j.

Now if $\mathfrak{q} \in \mathbb{V}((x_1, \ldots, x_i, x_{i+1}))$ we have $\mathfrak{p} \subseteq \mathfrak{q}$ for some $\mathfrak{p} \in \operatorname{Min}(x_1, \ldots, x_i)$. If $\operatorname{height}(\mathfrak{p}) \geq i+1$ then $\operatorname{height}(\mathfrak{q}) \geq i+1$. If $\operatorname{height}(\mathfrak{p}) = i$ then $\mathfrak{p} = \mathfrak{p}_j$ for some j and thus $x_{i+1} \notin \mathfrak{p}$. Hence $\mathfrak{p} \subsetneq \mathfrak{q}$ and so $\operatorname{height}(\mathfrak{q}) \geq \operatorname{height}(\mathfrak{p}) + 1 = i + 1$.

Now since $\operatorname{height}(x_1, \ldots, x_d) = d = \operatorname{height}(\mathfrak{m})$ we have that $\mathbb{V}(x_1, \ldots, x_d) = \{\mathfrak{m}\}$ and so $\sqrt{(x_1, \ldots, x_d)} = \mathfrak{m}$. Since its radical is the maximal ideal $\mathfrak{m}$, we conclude that $(x_1, \ldots, x_d)$ is $\mathfrak{m}$-primary. □

April 26, 2021

To prove the remaining inequality in the dimension theorem we need one additional lemma.

Lemma 5.73. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. If x is a non zero-divisor in R and $R' = R/(x)$ then $d(R') \leq d(R) - 1$.*

Proof. There is a short exact sequence

$$0 \to (x) \to R \to R/(x) \to 0.$$

We consider the $\mathfrak{m}$-adic filtration $\mathcal{F} = \{\mathfrak{m}^n\}_{n \geq 0}$ on R and the induced filtration on (x), $\mathcal{F}' = \{(x) \cap \mathfrak{m}^n\}_{n \geq 0}$. For each $n \in \mathbb{N}$ these fit into another short exact sequence

$$0 \to \frac{(x)}{(x) \cap \mathfrak{m}^n} \to \frac{R}{\mathfrak{m}^n} \to \frac{R}{(x) + \mathfrak{m}^n} \to 0$$

or

$$0 \to \frac{(x)}{(x) \cap \mathfrak{m}^n} \to \frac{R}{\mathfrak{m}^n} \to \frac{R'}{\overline{\mathfrak{m}}^n} \to 0.$$

Additivity of length in short exact sequences yields

$$\chi_{\mathfrak{m}}^{R}(n) = \ell\left(\frac{(x)}{(x) \cap \mathfrak{m}^n}\right) + \chi_{\mathfrak{m}}^{R'}(n) \tag{5.3}$$

By the Artin-Rees Lemma there is $k \in \mathbb{N}$ so that

$$(x) \cap \mathfrak{m}^n = \mathfrak{m}^{n-k}((x) \cap \mathfrak{m}^k) \text{ for } n \geq k$$

and thus there are containments

$$\mathfrak{m}^n(x) \subseteq (x) \cap \mathfrak{m}^n \subseteq \mathfrak{m}^{n-k}(x)$$

which yield inequalities

$$\ell\left(\frac{(x)}{\mathfrak{m}^n(x)}\right) \geq \ell\left(\frac{(x)}{(x) \cap \mathfrak{m}^n}\right) \geq \ell\left(\frac{(x)}{\mathfrak{m}^{n-k}(x)}\right).$$

Since x is a non zero-divisor in R, the map $R \to (x)$ sending $1 \mapsto x$ is an R-module isomorphism. Since $(x) \cong R$, the inequalities above can be rewritten as

$$\chi^R_{\mathfrak{m}}(n) \geq \ell\left(\frac{(x)}{(x) \cap \mathfrak{m}^n}\right) \geq \chi^R_{\mathfrak{m}}(n-k).$$

This shows that the function $n \mapsto \ell\left(\frac{(x)}{(x)\cap \mathfrak{m}^n}\right)$, which is eventually polynomial, has the same degree, $d(R)$, and same leading coefficient as $\chi^R_{\mathfrak{m}}$.

From (5.3) we now see that the function $\chi^{R'}_{\mathfrak{m}}(n)$ is eventually equal to a polynomial of degree strictly smaller than $d(R)$. □

Proposition 5.74. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. Then $d(R) \geq \dim(R)$.*

Proof. By induction on $d = d(R)$.

If $d = 0$ then $\ell(R/\mathfrak{m}^n)$ is constant for $n \gg 0$. Since $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \ell(R/\mathfrak{m}^n) - \ell(R/\mathfrak{m}^{n+1})$, we see that $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$ for $n \gg 0$ which means $\mathfrak{m}^n/\mathfrak{m}^{n+1} = 0$ or $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for $n \gg 0$. By Nakayama's lemma we have $\mathfrak{m}^n = 0$ for $n \gg 0$. Thus R is artinian by Proposition 5.27 and so $\dim(R) = 0$.

Suppose $d > 0$ and let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain of primes in R. Let $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$. Let $R' = R/\mathfrak{p}_0$, a local ring with maximal ideal $\mathfrak{m}' = \mathfrak{m}/\mathfrak{p}_0$. Let $\overline{x}$ be the image of x in R'. Since R' is a domain, $\overline{x}$ is a non zero-divisor. By the previous lemma we have $d(R'/(\overline{x})) \leq d(R') - 1$.

Since there is a surjection $R/\mathfrak{m}^n \twoheadrightarrow R'/\mathfrak{m}'^n$ we have

$$\chi^R_{\mathfrak{m}}(n) = \ell_R(R/\mathfrak{m}^n) \geq \ell_{R'}(R'/\mathfrak{m}'^n) = \chi^{R'}_{\mathfrak{m}}(n).$$

(Recall that length is the same as vector space dimension over both R and R'). This shows the first inequality in the sequence

$$d = d(R) \geq d(R') \geq d(R'/(\overline{x})) + 1 \geq \dim(R'/(\overline{x})) + 1.$$

The second inequality follows from Lemma 5.73 and the third is from the inductive hypothesis applied to $R'/(\overline{x})$). To summarize, the above inequality shows $\dim(R'/(\overline{x})) \leq d - 1$.

The images of $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in $R'/(\overline{x})$) form a chain of length $r - 1$, so that $r - 1 \leq d - 1$. This shows that $r \leq d$ and taking the maximum of such r yields the desired conclusion $\dim(R) \leq d$. □

WE have now established the Dimension Theorem.

Proof of the Dimension Theorem 5.68. It follows from Theorem 5.66, Proposition 5.72, and Proposition 5.74. □

The definition of $\delta(R)$ singles out the M-primary ideals with $\dim(R)$ generators. A set of minimal generators for such an ideal has a special name

Definition 5.75. Let $(R, \mathfrak{m}, k)$ be a noetherian local ring with $\dim(R) = d$. A *system of parameters*, abbreviated s.o.p., for R is a set of elements $x_1, \ldots, x_d \in R$ so that

$$\sqrt{(x_1, \ldots, x_d)} = \mathfrak{m}.$$

As a consequence of the Dimension Theorem every noetherian local ring has a system of parameters (in fact it has many). Systems of parameters are closely related to Noether normalization: it turns out that if R is a K-algebra then $x_1, \ldots, x_d$ is an s.o.p. for R if and only if $K[x_1, \ldots, x_d]$ is a Noether normalization for R.

Here are some very important consequences of the Dimension Theorem:

Theorem 5.76 (Generalized Principal Ideal Theorem)**.** *Let R be a noetherian ring, and $x_1, \ldots, x_r \in R$. Then* $\operatorname{height}(x_1, \ldots, x_r) \leq r$.

Proof. Let $\mathfrak{p} \in \operatorname{Min}((x_1, \ldots, x_r))$. Then $R_\mathfrak{p}$ is a noetherian local ring and $\mathbb{V}((x_1, \ldots, x_r)R_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\}$. This implies that $\sqrt{(x_1, \ldots, x_r)R_\mathfrak{p}} = \mathfrak{p}R_\mathfrak{p}$ and hence $(x_1, \ldots, x_r)R_\mathfrak{p}$ is $\mathfrak{p}R_\mathfrak{p}$-primary. Now we deduce from the Dimension Theorem that $r \geq \delta(R_\mathfrak{p}) = \operatorname{height}(\mathfrak{p})$. □

A famous corollary of this is

Corollary 5.77 (Krull's Principal Ideal Theorem)**.** *Let R be a noetherian ring. For any $x \in R$ we have* $\operatorname{height}(x) \leq 1$.

April 29, 2021

5.6 Regular local rings

The dimension theorem provides a useful bound on dimension of a local ring: the dimension is less or equal to the number of generators of the maximal ideal. We study the rings for which equality holds.

Corollary 5.78. *Let $(R, \mathfrak{m}, k)$ be a noetherian local ring. Then* $\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$.

Proof. We deduce from the Dimension Theorem that $\dim(R) = \delta(R) \leq \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$, where the last equality follows from Nakayama's lemma. □

We shall consider the case of equality, that is $\dim(R) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$, in the next section.

Definition 5.79. A noetherian local ring $(R, \mathfrak{m}, k)$ is *regular* if $\dim(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. A noetherian ring R is called *regular* if $R_\mathfrak{m}$ is a regular local ring for all maximal ideals $\mathfrak{m}$.

Example 5.80.
- A local ring $(R, \mathfrak{m})$ with $\dim R = 0$ is regular if and only if R is a field since we must have $\mu(\mathfrak{m}) = \dim R = 0$ so $\mathfrak{m} = (0)$.

- For any prime integer p, $\mathbb{Z}_{(p)}$ is a regular local ring since its dimension is one and its maximal ideal is principal. It follows that $\mathbb{Z}$ is regular.
- $K[x_1, \ldots, x_d]_{(x_1-a_1,\ldots,x_n-a_n)}$ is a regular local ring, since its dimension is n (equidimensionality) and its maximal ideal is generated by n elements. It follows that $K[x_1, \ldots, x_d]$ is regular, at least when K is algebraically closed. This is also the case for arbitrary K.
- If $R = K[x_1, \ldots, x_n], \mathfrak{m} = (x_1, \ldots, x_n)$ and $f \in R_1$ then $R/(f) \cong K[x_1, \ldots, x_{n-1}]$ is regular. But if $f \in R_+^2$ then $R/(f)$ is not regular since we have $\dim(R/(f))_{\overline{\mathfrak{m}}} = n-1$ but $\dim_k \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 = n$.

The last example explains some geometric phenomena that we have seen earlier in the course: consider the equation of a line L in $\mathbb{A}_K^2$, i.e. set $f = ax+by+c \notin R_+^2$. Then $R/(f) = K[L]$ is a regular ring. We can see this geometrically as saying that every point on the line L is smooth (more about what this word means later). On the other hand let f be the equation of the cuspidal curve 2.40 $f = y^2 - x^3$ or the nodal curve 2.41 $f = y^2 + x^2(x-1)$. In either case we have $f \in R_+$ so if Z is the cusp or the nodal cubic then $K[Z] = R/(f)$ is not regular. This gives an easy way to see that L (which is isomorphic to $\mathbb{A}_K^1$) cannot be isomorphic to Z, since the respective coordinate rings cannot be isomorphic.

April 31, 2021

The Jacobian criterion

We want to give now the geometric idea behind the notion of a regular local ring. We first need to discuss the notion of tangent space.

Consider the graph of a function $y = f(x)$. Let $(a, f(a))$ be a point on this graph. Then the tangent line to the graph at the point $(a, f(a))$ has equation

$$y = f(a) + f'(a)(x - a).$$

One could consider the above mentioned graph as an algebraic set $V(f(x)-y)$, and set $g(x, y) = f(x) - y$. Rewriting the equation of the tangent line in this notation yields

$$\frac{\partial g}{\partial x}(a)(x - a) + \frac{\partial g}{\partial y}(a)(y - f(a)) = 0.$$

The left hand side of the equation above is the linear approximation (linear part of the Taylor series) of $g(x, y)$ at $(a, f(a))$.

More generally, we have

Definition 5.81. If $X = V(I) \subseteq \mathbb{A}^n$ with $I = (f_1, \ldots, f_s)$ and $\underline{a} = (a_1, \ldots, a_n) \in X$ then the *tangent space* to X at $\underline{a}$ is

$$T_{X,\underline{a}} = V\left(\sum_{j=1}^{n} \frac{\partial f_1}{\partial x_j}(\underline{a})(x_j - a_j), \ldots, \sum_{j=1}^{n} \frac{\partial f_s}{\partial x_j}(\underline{a})(x_j - a_j)\right).$$

Remark 5.82. Tangent spaces are affine subspaces of $\mathbb{A}^n = k^n$. The vector space dimension of $T_{X,\underline{a}}$ is $\dim_k(T_{X,\underline{a}}) = n - \operatorname{rank}(J)$ where J is the matrix of coefficients of the linear system in Definition 5.81

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_s}{\partial x_1} & \cdots & \frac{\partial f_s}{\partial x_n} \end{bmatrix}.$$

This matrix is called the *Jacobian matrix* of $I = (f_1, \ldots, f_s)$.

Definition 5.83. One says that X is *smooth* at a or a is a smooth point of X if the dimension of the tangent space $T_{X,\underline{a}}$ (as a vector space or algebraic variety - they are the same) is equal to the dimension of the coordinate ring of the algebraic variety X. A point that is not smooth is called *singular*.

We are now ready for the geometric interpretation of regular rings.

Theorem 5.84. *Let X be an algebraic variety, consider a point $\underline{a} = (a_1, \ldots, a_n) \in X$ with maximal ideal $\mathfrak{m}_{\underline{a}}$ (note that $I \subseteq \mathfrak{m}_{\underline{a}}$) and coordinate ring*

$$R = K[x_1, \ldots, x_n]/I.$$

The following are equivalent

1. *$R_{\mathfrak{m}_{\underline{a}}}$ is a regular local ring*
2. *$\underline{a}$ is a smooth point of X, i.e. $\dim(R) = \dim_k(T_{X,\underline{a}})$*
3. *the rank of the Jacobian matrix of I evaluated at $\underline{a}$ is equal to $\operatorname{height}(I)$.*

Proof. We first see that the image of $f \in \mathfrak{m}_{\underline{a}}$ in $\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2$ is the linear part of the Taylor series of f, by using Taylor's formula to write

$$f = \underbrace{f(\underline{a})}_{0} + \sum_j \frac{\partial f_i}{\partial x_j}(\underline{a})(x_j - a_j) + g \text{ with } g \in \mathfrak{m}^2.$$

Note also that a basis for $\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2$ is given by $\{\overline{x_1 - a_1}, \ldots, \overline{x_n - a_n}\}$ so we can identify the image of f in $\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2$ written in this basis with the vector $\nabla_{\underline{a}}(f) = (\frac{\partial f_i}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$. This shows that the subspace of $\mathbb{A}_K^n$ spanned by $\nabla_{\underline{a}}(f_1), \ldots, \nabla_{\underline{a}}(f_t)$ is isomorphic to the subspace of $\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2$ given by the images of the f_i's.

Now, let $\mathfrak{m} = \mathfrak{m}_{\underline{a}}/I$ be the maximal ideal of R. We have that $\mathfrak{m}/\mathfrak{m}^2 \cong (\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2)/(I/\mathfrak{m}_{\underline{a}}^2)$ and $I/\mathfrak{m}_{\underline{a}}^2 = \operatorname{Span}_K\{\overline{f_1}, \ldots, \overline{f_t}\}$ hence

$$\begin{aligned} \dim_K(\mathfrak{m}/\mathfrak{m}^2) &= \dim_K(\mathfrak{m}_{\underline{a}}/\mathfrak{m}_{\underline{a}}^2) - \operatorname{Span}_K\{\overline{f_1}, \ldots, \overline{f_t}\} \\ &= n - \dim_K \operatorname{Span}_K\{\nabla_{\underline{a}}(f_1), \ldots \nabla_{\underline{a}}(f_t)\} \\ &= \dim T_{X,\underline{a}}. \end{aligned}$$

Since R is a K-algebra domain all chains from (0) to any maximal ideal in R have the same length, so the following formula holds

$$\dim(R) = \dim R_{\mathfrak{m}_{\underline{a}}}.$$

Also, denoting $\text{height}(I) = h$ we have

$$\dim(R) = \dim K[x_1, \ldots, x_n] - \text{height}(I) = n - h.$$

We now find that $\dim(R) = \dim_K(\mathfrak{m}/\mathfrak{m}^2) \iff \dim(R) = \dim T_{X,\underline{a}} \iff$

$$n - h = n - \dim_K \text{Span}_K\{\nabla_{\underline{a}}(f_1), \ldots \nabla_{\underline{a}}(f_t)\} \iff$$

$$h = \dim_K \text{Span}_K\{\nabla_{\underline{a}}(f_1), \ldots \nabla_{\underline{a}}(f_t)\} = \text{rank}\, J(\underline{a}).$$

□

Example 5.85.

1. Let $R = \mathbb{C}[x, y]/(y^2 - x^3)$. The matrix J is $[2x, 3y^2]$, which shows that the only non-smooth point of the cuspidal cubic curve is $V(2x, 3y^2) = (0, 0)$. Notice that the tangent space to the cuspidal cubic at $(0, 0)$ is $\mathbb{A}^2_K$ while at every other point it is a 1-dimensional subspace of $\mathbb{A}^2_K$.

2. Similarly for $R = \mathbb{C}[x, y]/(y^2 - x^2(x + 1))$ the matrix J is $[-3x^2 - 2x, y]$, which shows that the only non-smooth points of the nodal curve are the zero set of the ideal $(-3x^2 - 2x, y) = (x, y) \cap (-3x - 2, y)$. Thus this curve has two singular points: $(0, 0)$ and $(-2/3, 0)$.

Chapter 6

Where next?

In this course, we have studied classical commutative algebra and a bit of affine geometry. To get an idea of what this work encompasses in the realm of time, here are the main figures whose contributions we have been learning about:

- David Hilbert (1862-1943)
- Emmy Noether (1882-1935)
- Wolfgang Krull (1899-1971)
- Oskar Zariski (1899-1986)

Most of the material which we have studied was developed at the end of the 19-th century and the in the first half of the 20-th century. However, there is much more to commutative algebra and its connections to related disciplines have evolved tremendously since then.

The following are the three main directions which build upon the material presented in these notes:

1. **Modern commutative algebra** is concerned with classes of rings which are not as restrictive as regular local rings, but maintain some of the nice properties that these rings have. These classes of rings fit into the following taxonomy:

   > Regular rings $\subseteq$ Complete Intersection rings $\subseteq$ Gorenstein rings $\subseteq$ Cohen-Macaulay rings.

   Several of these classes are defined by their homological properties (see item 2). A good place to learn about these rings is the book *Cohen-Macaulay rings* by Bruns and Herzog.

2. **Homological algebra** is concerned with methods that are widely applicable in algebra, geometry and topology and which generally revolve around the use of complexes. A good place to learn further methods of homological algebra is the book by the same name by Weibel.

3. **Modern algebraic geometry** is primarily concerned with algebraic sets in projective (as opposed to affine) spaces as well as their generalizations called schemes. These correspond to homogeneous ideals of the polynomial ring and their coordinate rings are graded rings. There are also geometric objects called sheaves which correspond to graded modules over these rings. Generally speaking the algebra-geometry dictionary is much enrich by the introduction of schemes and sheaves. Learning this entire dictionary takes a lot of dedication and patience in addition to the strong foundations in commutative algebra that we have developed. Some good references are the text books by Safarevich and Hartshorne and the course notes by Vakil.

Index

I-filtration, 86
I-stable filtration, 86
S_n, 5
T-graded, 81
$V(I)$, 23
$\mathrm{Ass}_R(M)$, 47
$\mathrm{Min}(I)$, 44
$\mathbb{V}(I)$, 37
$\mathrm{adj}(B)$, 11
$\mathrm{gr}(R)$, 88
$\mathrm{gr}_I(R)$, 88
$\mid r \mid$, 81
$\mathfrak{p}$-primary ideal, 42
$\sum_{\gamma\in\Gamma} A\gamma$, 9
$\widehat{B_{ij}}$, 11
$h_R(t)$, 83

affine algebra, 34
affine space, 20
algebra generated by a set, 7
algebra-finite, 8
algebraic map, 30
algebraic set, 24
algebraic variety, 24
algebraically independent, 7
associated graded ring, 88
associated prime, 47
associated primes of an ideal, 47

catenary, 63
classical adjoint, 11
composition series, 76
contraction, 51
coordinate ring, 34
cuspidal curve, 32

degree, 81
degree-preserving, 82
dimension, 59

equation of integral dependence, 11
equivalent composition series, 76
extension, 51

fine grading, 82
finitely generated A-algebra, 8
finitely generated module, 9
free algebra, 7

Gaussian integers, 10
generates as a module, 9
generates as an algebra, 7
generic point, 38

height, 61
Hilbert function, 83
Hilbert function for local rings, 90
Hilbert polynomial, 86
Hilbert series, 83
Hilbert series for local rings, 90
Hilbert-Samuel function, 90
Hilbert-Samuel polynomial, 91
homogeneous element, 81
homogeneous ideal, 82

ideal radical, 26
integral closure of A in R, 11
integral element, 10
integral over A, 11

irreducible decomposition, 41
irreducible ideal, 41
irredundant primary decomposition, 44

Jacobian matrix, 97

Krull dimension, 59

local ring, 72
local ring of a point, 73
localization, 50

map on Spec, 39
maximal spectrum, 37
minimal generators, 75
minimal primary decomposition, 44
minimal prime, 44
module generated by a set, 9
module-finite, 9
morphism of algebraic sets, 30
mSpec, 37

nodal cubic, 32
Noether normalization, 69
noetherian module, 14
noetherian ring, 13
normal domain, 67
number of minimal generators, 75

primary decomposition, 44
primary ideal, 42
prime avoidance, 92
purely transcendantal, 21

radical ideal, 26
reduced, 34
Rees algebra, 87
regular, 95
regular map, 30
residue field, 72

saturated chain of primes, 60
simple module, 76
singular point, 97
Spec, 37
spectrum, 37
standard graded, 82
standard grading, 82
system of parameters, 95

tangent space, 96
topological space, 37
transcendence basis, 21
transcendence degree, 22

vanishing set, 23
variety, 24

weights, 82

Zariski closed, 37
Zariski topology, 37
zero set, 23