MATH 902 LECTURE NOTES, SPRING 2022

Contents

Lecture of January 19, 2022

In this class, all rings are assumed to be commutative, with associative multiplication and containing 1.

1. Finiteness conditions

1.1. **Finitely generated algebras.** We start by recalling a definition from last semester, specialized to the setting of commutative rings.

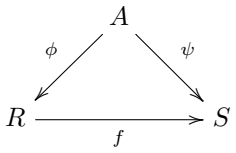
Definition 1.1 (Algebra)**.** Given a ring A, an *A-algebra* is a ring R equipped with a ring homomorphism $\phi : A \to R$. This defines an A-module structure on R given by restriction of scalars, that is, for $a \in A$ and $r \in R$, $ar := \phi(a)r$ that is compatible with the internal multiplication of R i.e.,

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

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

Example 1.2.
- If A is a ring and $x_1, \dots, x_n$ are indeterminates, the inclusion map $A \hookrightarrow A[x_1, \dots, x_n]$ makes the polynomial ring into an A-algebra.
- When $A \subseteq R$ the inclusion map makes R an A-algebra. In this case the A-module multiplication ar coincides with the internal (ring) multiplication on R.
- Any ring comes with a unique structure as a $\mathbb{Z}$-algebra.

The collection of A-algebras forms a category where the morphisms are ring homomorphisms $f : R \to S$ such that the following diagram commutes



for structural homomorphisms $\varphi : A \to R$ and $\psi : A \to S$.

Definition 1.3 (Algebra generation)**.** Let R be an A-algebra and let $\Lambda \subseteq R$ be a set. The *A-algebra generated by* a subset Λ of R, 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 $R = A[\Lambda]$.

Note that there are two different meanings for the notation $A[S]$ for a ring A and set S: one calls for a polynomial ring, and the other calls for a subring of something.

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

Lemma 1.4. *The following are equivalent*

(1) *Λ generates R as an A-algebra.*
(2) *Every element in R admits a polynomial expression in Λ with coefficients in $\phi(A)$, i.e.*

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

(3) *The A-algebra homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on a set of indeterminates X in bijection with Λ and $\psi(x_i) = \lambda_i$, is surjective.*

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

Example 1.5. We may have also seen these brackets used in $\mathbb{Z}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ to describe the ring

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

In fact, this is a special instance of generating: the $\mathbb{Z}$-algebra generated by $\sqrt{d}$ in the most natural place, the algebraic closure of $\mathbb{Q}$, is exactly the set above. The point is that for any power $(\sqrt{2})^n$, write $n = 2q + r$ with $r \in \{0, 1\}$, so $(\sqrt{2})^n = 2^d(\sqrt{2})^r$. Similarly, the ring $\mathbb{Z}[\sqrt[3]{d}]$ can be written as

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

Note that the homomorphism ψ in part (3) need not be injective.

- If the homomorphism ψ is injective (so an isomorphism) we say that A is a *free* algebra.
- the set $\ker(\psi)$ measures how far R is from being a free A-algebra and is called the set of *relations* on Λ.

Definition 1.6 (Algebra-finite)**.** We say that $\varphi : A \to R$ is *algebra-finite*, or R is a *finitely generated A-algebra*, if there exists a finite set of elements $f_1, \ldots, f_d$ that generates R as an A-algebra. We write $R = A[f_1, \ldots, f_d]$ to denote this.

The term *finite-type* is also used to mean this.

Remark 1.7. Note that, by the lemma on generating sets, an A-algebra is finitely generated if and only if it is isomorphic to a quotient of a polynomial ring over A in finitely many variables. The choice of an isomorphism with a quotient of a polynomial ring is equivalent to a choice of generating set.

Lecture of January 21, 2022

Example 1.8. Let K be a field, and $B = K[x, xy, xy^2, xy^3, \ldots] \subseteq C = K[x, y]$, where x and y are indeterminates. Let A be a finitely generated subalgebra of B, and write $A = K[f_1, \ldots, f_d]$. Since each f_i is a (finite) polynomial expression in the monomials $\{xy^i \mid i \in \mathbb{N}\}$, it involves only finitely many of these monomials. Thus, there is an m such that $\{f_1, \ldots, f_d\} \subset K[x, xy, \ldots, xy^m]$, and hence $A \subseteq K[x, xy, \ldots, xy^m]$. 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 K-algebra.

Optional Exercise 1.9. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms (so B is an A-algebra via ϕ, C is a B-algebra via ψ, and C is an A-algebra via $\psi \circ \phi$). Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are algebra-finite, then $A \xrightarrow{\psi\phi} C$ is algebra-finite. (Take the union of the generating sets.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $B \xrightarrow{\psi} C$ is algebra-finite. (Use the same generating set.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $A \xrightarrow{\phi} B$ may *not* be algebra-finite. (Use the previous example.)

Remark 1.10. Any surjective φ is algebra-finite: the target is generated by 1. Since any homomorphism $\phi : A \to R$ can be factored as $\phi = \psi \circ \varphi$ where φ is the surjection $\varphi : A \to A/\ker(\varphi)$ and ψ is the inclusion $\psi : A/\ker(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms by the last bullet point of the previous exercise.

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

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

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

1.2. **Finitely generated modules.** We will also find it quite useful to consider a stronger finiteness property for maps.

Definition 1.11. (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 1.12. *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.*
3. *The homomorphism $\theta : A^{\oplus Y} \to M$, where $A^{\oplus Y}$ is a free A-module with basis Y in bijection with Γ via $\theta(y_i) = \gamma_i$, is surjective.*

Optional Exercise 1.13. Prove the previous lemma.

Definition 1.14 (Module-finite)**.** We say that a ring homomorphism $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module, that is, there is a *finite* set $r_1, \ldots, r_n \in R$ so that $R = \sum_{i=1}^{n} Ar_i$.

As with algebra-finiteness, surjective maps are always module-finite in a trivial way. 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 1.15 (Module-finite $\Rightarrow$ algebra-finite)**.** *If $\varphi : A \to R$ is module-finite then it is algebra-finite.*

The converse is not true.

Example 1.16.

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

Optional Exercise 1.17. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms. Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are module-finite, then $A \xrightarrow{\psi\phi} C$ is module-finite.
- If $A \xrightarrow{\psi\phi} C$ is module-finite, then $B \xrightarrow{\psi} C$ is module-finite.

We will see that $A \xrightarrow{\psi\phi} C$ is module-finite does not imply $A \xrightarrow{\phi} B$ is module-finite soon.

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

Definition 1.18 (Integral element/extension)**.** Let $\phi : A \to R$ be a ring homomorphism (for which we will denote $\phi(a)$ by a) and $r \in R$. The element r is *integral* 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. The homomorphism ϕ is *integral* if every element of R is integral over A.

Example 1.19. Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. The element $t = \sqrt{2} \in A$ is integral over $\mathbb{Z}$, since $t^2 - 2 = 0$. Likewise, $s = 1 + \sqrt{2}$ is integral over $\mathbb{Z}$, as $s^2 = 3 + 2\sqrt{2}$, so $s^2 - 2s - 1 = 0$.

On the other hand, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$: if

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

with $a_i \in \mathbb{Z}$, multiply through by 2^n to get $1 + 2a_{n-1} + 2^2 a_{n-2} + \cdots + 2^n a_0 = 0$, which is impossible.

Lecture of January 24, 2022

Proposition 1.20. *Let $A \subseteq R$ be rings.*

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

Proof. (1) Suppose r is integral over A, 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, $s \in A[r]$ with a polynomial expression $s = p(r) = \sum c_j r^j$ of degree $m \geqslant n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in r.

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

We recall that the *classical adjoint* of an $n \times n$ matrix A is the $n \times n$ matrix whose (i, j)-entry is $(-1)^{i+j}$ times the determimant of the matrix obtained from A by removing the ith column and the jth row.

Lemma 1.21 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^{\oplus n}$, and $r \in R$.*

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

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

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

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

since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish

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

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

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

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

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

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

Theorem 1.22. *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

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

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

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

for each i. Let $C = [a_{ij}]$, and v be the column vector $(r_1, \ldots, r_t)$. We have $rv = Cv$, so by the determinant trick, $\det(rI_{n\times n} - C)v = 0$. Since we chose one of the entries of v to be 1, we have in particular that $\det(rI_{n\times n} - C) = 0$. Expanding this determinant as a polynomial in r, this is a monic equation with coefficients in A. $\square$

Collecting the previous results, we now have a useful characterization of module-finite extensions:

Corollary 1.23 (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): A generating set for R as an A-module serves as a generating set as an A-algebra. The remainder of this direction comes from the previous theorem. ($\Leftarrow$): If $R = A[r_1, \ldots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.20. $\square$

Corollary 1.24. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

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

For the latter statement, the first statement implies that

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

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

Example 1.25. (1) Not all integral extensions are module-finite. Let $K = \overline{K}$, and consider the ring

$$R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \dots] \subseteq \overline{K(x)}.$$

Clearly R is generated by integral elements over $K[x]$, hence integral, but is not algebra-finite over $K[x]$.

(2) Let x, y, z be indeterminates. Set $R = \mathbb{C}[x, y]$ to be a polynomial ring, and $S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$ to be a quotient of a polynomial ring. We claim that we can realize R as a subring of S; i.e., the $\mathbb{C}$-algebra homomorphism from R to S that sends x to x and y to y is injective. Indeed, the kernel is the set of polynomials in x, y that are multiples of $z^2 + x^2 + y^2$, but, thinking of $\mathbb{C}[x, y, z]$ as $R[z]$, any nonzero multiple of $z^2 + x^2 + y^2$ must have z-degree at least 2, so none only involve x, y. Thus, we have an inclusion $R \subseteq S$.

The ring S is module-finite over R: indeed, S is generated over R as an algebra by one element z that is integral over R.

Lecture of January 26, 2022

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

Example 1.27. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$: this follows from essentially the same argument we used to show that $\frac{1}{2}$ is not integral over $\mathbb{Q}$.

Optional Exercise 1.28. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is $\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4. \end{cases}$

Optional Exercise 1.29. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms. Then $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are integral if and only if $A \xrightarrow{\psi\phi} C$ is integral.

Here is a useful fact about integral extensions that we will use multiple times; it also gives a flavor for the power of the integrality condition on a map.

Proposition 1.30. *Let R and S be domains and $R \subseteq S$ be integral. Then R is a field if and only if S is a field.*

Proof. ($\Rightarrow$) Say $R = K$ is a field and let $s \in S$ be nonzero. The ring $K[s]$ is integral over K and algebra-finite, hence module finite; i.e., a finite dimensional vector space. Then multiplication by s on $K[s]$ is an injective K-linear map, since $K[s] \subseteq S$ is a domain, and hence surjective. This means that s has an inverse, and hence S is a field.

($\Leftarrow$) Say $S = L$ is a field and let $r \in R$. Then $r^{-1} \in L$ and is hence integral over R. Take an integral equation

$$(r^{-1})^n + a_1(r^{-1})^{n-1} + \cdots + a_n = 0$$

with $a_i \in R$, and multiply through by r^{n-1} to get

$$r^{-1} + a_1 + a_2 r + \cdots + a_n r^{n-1} = 0,$$

so $r^{-1} \in R$. □

1.4. **Commutative Noetherian rings and modules.** We recall that a ring R is *Noetherian* if the following equivalent conditions hold:

(1) The set of ideals of R has ACC (every ascending chain has a maximal element)
(2) Every nonempty collection of ideals of R has a maximal element (i.e., an ideal not contained in any other; not necessarily a maximal ideal though)
(3) Every ideal of R is finitely generated.

Similarly, a module M is *Noetherian* if the following equivalent conditions hold:

(1) The set of submodules of M has ACC (every ascending chain has a maximal element)
(2) Every nonempty collection of sumbodules of M has a maximal element
(3) Every submodule of M is finitely generated.

When R is Noetherian, a module is finitely generated if and only if it is Noetherian, and hence every submodule of a finitely generated module is finitely generated.

Example 1.31.
(1) If K is a field, the only ideals in K are (0) and $(1) = K$, so K is a Noetherian ring.
(2) $\mathbb{Z}$ is a Noetherian ring. More generally, if R is a PID, then R is Noetherian. Indeed, every ideal is finitely generated!
(3) As a special case of the previous example, consider the ring of germs of complex analytic functions near 0,
$$\mathbb{C}\{z\} := \{f(z) \in \mathbb{C}[\![z]\!] \mid f \text{ is analytic on a neighborhood of } z = 0\}.$$
This ring is a PID: every ideal is of the form (z^n), since any $f \in \mathbb{C}\{z\}$ can be written as $z^n g(z)$ for some $g(z) \neq 0$, and any such $g(z)$ is a unit in $\mathbb{C}\{z\}$.
(4) A ring that is *not* Noetherian is a polynomial ring in infinitely many variables over a field k, $R = k[x_1, x_2, \ldots]$: the ascending chain of ideals
$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$$
does *not* stabilize.
(5) The ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots]$ is also *not* Noetherian. A nice ascending chain of ideals is
$$(x) \subsetneqq (x^{1/2}) \subsetneqq (x^{1/3}) \subsetneqq (x^{1/4}) \subsetneqq \cdots.$$
(6) The ring of continuous real-valued functions $\mathcal{C}(\mathbb{R}, \mathbb{R})$ is *not* Noetherian: the chain of ideals
$$I_n = \{f(x) \mid f|_{[-1/n, 1/n]} \equiv 0\}$$
is increasing and proper. The same construction shows that the ring of infinitely differentiable real functions $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ is not Noetherian: properness of the chain follows from, e.g., Urysohn's lemma (though it's not too hard to find functions distinguishing the ideals in the chain). Note that if we asked for analytic functions instead of infinitely-differentiable functions, every element of the chain would be the zero ideal!

Remark 1.32. If R is Noetherian and $I \subseteq R$, then R/I is Noetherian as well, since there is an order-preserving bijection

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

Definition 1.33. If R is a commutative ring and x is an indeterminate the set

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

with the obvious addition and multiplication is called the *power series ring* in the variable x with coefficients in R. If $x_1, \ldots, x_d$ are distinct indeterminates the *power series ring* in all of these variables is defined inductively as

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

We will now give a huge family of Noetherian rings.

Theorem 1.34 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then the rings $R[x_1, \ldots, x_d]$ and $R[\![x_1, \ldots, x_d]\!]$ are Noetherian.*

Proof. We give the proof for polynomial rings, and indicate the difference in the power series argument. By induction on d, we can reduce to the case $d = 1$. Given $I \subseteq R[x]$, let

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

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

Given any $f \in I$ of degree greater than N, we can cancel off the leading term of f by subtracting a suitable combination of the f_i, so any $f \in I$ can be written as $f = g + h$ where $h \in (f_1, \ldots, f_t)$ and $g \in I$ has degree at most N, so $g \in I \cap (R + Rx + \cdots + Rx^N)$. Note that since $I \cap (R + Rx + \cdots + Rx^N)$ is a submodule of the finitely generated free R-module $R + Rx + \cdots + Rx^N$, it is also finitely generated as an R-module. Given such a generating set, say $I \cap (R + Rx + \cdots + Rx^N) = (f_{t+1}, \ldots, f_s)$, we can write any such $f \in I$ as an $R[x]$-linear combination of these generators and the f_i's. Therefore, $I = (f_1, \ldots, f_t, f_{t+1}, \ldots, f_s)$ is finitely generated, and $R[x]$ is a Noetherian ring.

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

Corollary 1.35. *If R is Noetherian, then any finitely generated R-algebra is Noetherian as well.*

Proof. A finitely generated R-algebra is a quotient ring of a polynomial ring in finitely many variables over R. □

Note that the converse to this is false, e.g., a power series ring over a field is Noetherian, but is not a finitely generated algebra.

Lecture of January 28, 2022

We now give a subtle connection between the finiteness conditions discussed.

Theorem 1.36 (Artin-Tate Lemma)**.** *Let $A \subseteq B \subseteq C$ be rings. Assume that*

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

Then, B is algebra-finite over A.

Proof. Let $C = A[f_1, \dots, f_r]$ and $C = Bg_1 + \cdots + Bg_s$. Then,

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

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

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

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

1.5. **Application: Finite generation of rings of invariants.** Historically, commutative algebra has roots in classical questions of algebraic and geometric flavors, including the following natural question:

Question 1. *Given a (finite) set of symmetries, consider the collection of polynomial functions that are fixed by all of those symmetries. Can we describe all the fixed polynomials in terms of finitely many of them?*

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

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

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

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

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

Question 2. *Given a finite group G acting on $R = K[x_1, \dots, x_d]$, is R^G a finitely generated K-algebra?*

Observe that, in this setting, R^G is a K-subalgebra of R, which is a finitely generated K-algebra, but this does not guarantee a priori that R^G is a finitely generated K-algebra.

Example 1.37 (Negative variables)**.** Let $G = \{e, g\}$ act on $R = K[x]$ by negating the variable: $g \cdot x = -x$ for all i, so $g \cdot f(x) = f(-x)$. Suppose that the characteristic of K is not 2, so $-1 \neq 1$. Write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. We have $g \cdot x^i = (-x)^i = (-1)^i x^i$, so

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

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

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

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

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

Optional Exercise 1.38. Generalize the last example as follows: let K be a filed with a primitive dth root of unity ζ, and let $G = \langle g \rangle \cong C_d$ act on $K[x_1, \ldots, x_n]$ via $g \cdot x_i = \zeta x_i$ for all i. Then

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

Example 1.39 (Standard representation of the symmetric group)**.** Let S_n be the symmetric group on n letters acting on $R = K[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$.

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

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

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

E.g, f above is $e_1^2 - 2e_2$. (Moreover, any symmetric polynomial can be written like so in a *unique* way, so R^{S_n} is a free K-algebra.) So even though we have infinitely many invariant polynomials, we can understand them in terms of only finitely many of them, which are *fundamental* invariants.

Proposition 1.40. *Let K be a field, R be a finitely-generated K-algebra, and G a finite group of automorphisms of R that fix K. Then $R^G \subseteq R$ is module-finite.*

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

First, since R is generated by a finite set as a K-algebra, and $K \subseteq R^G$, it is generated by the same finite set as an R^G-algebra as well. Extend the action of G on R to $R[t]$ with G fixing t. Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g \in G}(t - g(r)) \in R[t]$. Then G fixes $F_r(t)$, since for each $h \in G$,

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

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

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

Therefore, $F_r(t) \in R^G[t]$. The leading term (with respect to t) of $F_r(t)$ is $t^{|G|}$, so $F_r(t)$ is monic, and r is integral over R^G. Therefore, R is integral over R^G. □

Theorem 1.41 (Noether's finiteness theorem for invariants of finite groups)**.** *Let K be a field, R be a polynomial ring over K, and G be a finite group acting K-linearly on R. Then R^G is a finitely generated K-algebra.*

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

Lecture of January 31, 2022

2. Graded rings

2.1. **Basics of graded rings.** When we think of a polynomial ring R, we often think of R with its graded structure, in terms of degrees of elements. Other rings we have seen also have a graded structure, and this structure is actually very powerful.

Definition 2.1. An $\mathbb{N}$-*graded ring* is a ring R equipped with a direct sum decomposition as additive groups

$$R = \bigoplus_{a \geqslant 0} R_a,$$

such that $R_a R_b \subseteq R_{a+b}$ for every $a, b \in \mathbb{N}$, meaning that for any $r \in R_a$ and $s \in R_b$, we have $rs \in R_{a+b}$.

We say R is a *positively graded A-algebra* if R is $\mathbb{N}$-graded with $R_0 = A$.

More generally, for a semigroup T, a T-*graded* ring is a ring R with a direct sum decomposition of R as an additive group indexed by T:

$$R = \bigoplus_{a \in T} R_a$$

satisfying $R_a R_b \subseteq R_{a+b}$. We will assume for convenience that any grading semigroup is cancellative.

An element that lies in one of the summands R_a is said to be *homogeneous* of *degree* a; we write $|r|$ or $\deg(r)$ to denote the degree of a homogeneous element r.

By definition, an element in a graded ring is uniquely a sum of homogeneous elements, which we call its *homogeneous components* or *graded components*; we may write $[f]_d$ for the dth homogeneous component of f. One nice thing about graded rings is that many properties can usually be sufficiently checked on homogeneous elements, and these are often easier to deal with.

Lemma 2.2. *Let R be a T-graded ring.*

1. *1 is homogeneous of degree $0 \in T$ (the identity of T).*
2. *R_0 is a subring of R.*
3. *Each R_a is a R_0-module.*

Proof. (1) Write $1 = \sum_a r_a$ with r_a homogeneous of degree a. Then $r_0 = r_0(\sum_a r_a) = \sum_a r_0 r_a$ implies $r_0 r_a = 0$ for $a \neq 0$. Similarly, taking the R_a component of $r_a = r_a(\sum_b r_b)$ yields $r_a = r_a r_0$ (here is where we use the cancellative assumption). Thus $r_a = 0$ for $a \neq 0$, so $1 \in R_0$.

(2) R_0 is a subgroup under addition, and $r, s \in R_0$ implies $rs \in R_0$. We also just showed $1 \in R_0$.

(3) R_a is a subgroup under addition, and $r \in R_0$, $s \in R_a$ implies $rs \in R_a$.

□

Remark 2.3. Note that whenever R is a graded ring, the multiplicative identity 1 must be a homogeneous element whose degree is the identity in T. In particular, if R is $\mathbb{N}$ or $\mathbb{Z}$-graded, then $1 \in R_0$ and R_0 is a subring of R.

Example 2.4. Let K be a field, and $R = K[x_1, \ldots, x_n]$ be a polynomial ring.

(1) There is an $\mathbb{N}$-grading on R called the *standard grading* where

$$R_d = K \cdot \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \sum_i \alpha_i = d\}.$$

Of course, this is the notion of degree familiar from grade school. So $x_1^2 + x_2 x_3$ is homogeneous in the standard grading, while $x_1^2 + x_2$ is not.

(2) We can give different $\mathbb{N}$-gradings on R by fixing some tuple $(\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ and letting x_i be a homogeneous element of degree β_i; we call this a grading with *weights* $(\beta_1, \dots, \beta_n)$. Concretely,

$$R_d = K \cdot \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \sum_i \beta_i \alpha_i = d\}.$$

For example, in $K[x_1, x_2]$, $x_1^2 + x_2^3$ is not homogeneous in the standard grading, but it is homogeneous of degree 6 under the $\mathbb{N}$-grading with weights $(3, 2)$.

(3) A polynomial ring $R = K[x_1, \dots, x_n]$ also admits a natural $\mathbb{N}^n$-grading, with

$$R_{(d_1,\dots,d_n)} = K \cdot x_1^{d_1} \cdots x_n^{d_n}.$$

This is called the *fine grading*.

Definition 2.5. An ideal I in a graded ring R is called *homogeneous* if it can be generated by homogeneous elements.

Lemma 2.6. *Let I be an ideal in a graded ring R. The following are equivalent:*

(1) *I is homogeneous.*
(2) *For any element $f \in R$ we have $f \in I$ if and only if every homogeneous component of f lies in I.*
(3) *$I = \bigoplus_{a \in T} I_a$, where $I_a = I \cap R_a$.*

Proof. (1) $\Rightarrow$ (2): If I is homogeneous and $f \in I$, write f as a combination of the (homogeneous) generators of I, say $f_1, \dots, f_n$:

$$f = r_1 f_1 + \cdots + r_n f_n.$$

Write each r_i as a sum of its components, say $r_i = [r_i]_{d_{i,1}} + \cdots + [r_i]_{d_{i,m_i}}$. Then, after substituting and collecting,

$$f = \sum_d ([r_1]_{d-|f_1|} f_1 + \cdots + [r_n]_{d-|f_n|} f_n)$$

expresses f as a sum of homogeneous elements of different degrees, so

$$f_d = [r_1]_{d-|f_1|} f_1 + \cdots + [r_n]_{d-|f_n|} f_n \in I.$$

(2) $\Rightarrow$ (1): Any element of I is a sum of its homogeneous components. Thus, in this case, the set of homogeneous elements in I is a generating set for I.

(2) $\Rightarrow$ (3): As above, I is generated by the collection of additive subgroups $\{I_a\}$ in this case; the sum is direct as there is no nontrivial $\mathbb{Z}$-linear combination of elements of different degrees.

(3) $\Rightarrow$ (2): Clear. □

Example 2.7. Given an $\mathbb{N}$-graded ring R, then $R_+ = \bigoplus_{d>0} R_d$ is a homogeneous ideal.

We now observe the following:

Lemma 2.8. *Let R be an T-graded ring, and I be a homogeneous ideal. Then R/I has a natural T-graded structure induced by the T-graded structure on R.*

Proof. The ideal I decomposes as the direct sum of its graded components, so we can write

$$R/I = \frac{\oplus R_a}{\oplus I_a} \cong \oplus \frac{R_a}{I_a}.$$ □

Example 2.9. (1) The ideal $I = (w^2x + wyz + z^3, x^2 + 3xy + 5xz + 7yz + 11z^2)$ in $R = K[w, x, y, z]$ is homogeneous with respect to the standard grading on R, and thus the ring R/I admits an $\mathbb{N}$-grading with $|w| = |x| = |y| = |z| = 1$.

(2) In contrast, the ring $R = k[x, y, z]/(x^2 + y^3 + z^5)$ does not admit a grading with $|x| = |y| = |z| = 1$, but does admit a grading with $|x| = 15, |y| = 10, |z| = 6$.

Definition 2.10. Let R be a T-graded ring. A graded R-module is an R-module with a direct sum decomposition as additive groups indexed by T:

$$M = \bigoplus_{a \in T} M_a \text{ such that } R_a M_b \subseteq M_{a+b}$$

for all $a, b \in T$.

The notions of homogeneous element of a module and degree of a homogeneous element of a module take the obvious meanings. A notable abuse of notation: we will often talk about $\mathbb{Z}$-graded modules over $\mathbb{N}$-graded rings, and likewise.

We can also talk about graded homomorphisms.

Definition 2.11. Let R and S be T-graded rings with the same grading monoid T. A ring homomorphism $\phi : R \to S$ is *graded* or *degree-preserving* if $\phi(R_a) \subseteq S_a$ for all $a \in T$.

Note that our definition of ring homomorphism requires $1_R \mapsto 1_S$, and thus it does not make sense to talk about graded ring homomorphisms that shift degrees. But we can have graded module homomorphisms of any degree.

Definition 2.12. Let M and N be $\mathbb{Z}$-graded modules over the $\mathbb{N}$-graded ring R. A homomorphism of R-modules $\varphi : R \to S$ is *graded* if $\varphi(M_a) \subseteq N_{a+d}$ for all $a \in \mathbb{Z}$ and some fixed $d \in \mathbb{Z}$, called the *degree* of φ. A graded homomorphism of degree 0 is also called *degree-preserving*.

Example 2.13. Let K be a field, and let $R = K[x_1, \ldots, x_n]$ be a polynomial ring with the standard grading. Given $c \in K = R_0$, the homomorphism of R-modules $R \to R$ given by $f \mapsto cf$ is degree preserving. However, if instead we take $g \in K = R_d$ for some $d > 0$, then the map

$$\begin{aligned} R &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is not degree preserving, although it is a graded map of degree d. We can make this a degree-preserving map if we shift the grading on R by defining $R(-d)$ to be the R-module R but with the $\mathbb{Z}$-grading given by $R(-d)_t = R_{t-d}$. With this grading, the component of degree d of $R(-d)$ is $R(-d)_d = R_0 = K$. Now the map

$$\begin{aligned} R(-d) &\longrightarrow R \\ f &\longmapsto gf \end{aligned}$$

is degree preserving.

Lecture of February 2, 2022

We observed earlier an important relationship between algebra-finiteness and Noetherianity that followed from the Hilbert basis theorem: if R is Noetherian, then any algebra-finite extension of R is also Noetherian. There isn't a converse to this in general: there are lots of algebras over fields K that are Noetherian but not algebra-finite over K. However, for graded rings, this converse relation holds.

Proposition 2.14. *Let R be an $\mathbb{N}$-graded ring, and consider homogeneous elements $f_1, \ldots, f_n \in R$ of positive degree. Then $f_1, \ldots, f_n$ generate the ideal $R_+ := \bigoplus_{d>0} R_d$ if and only if $f_1, \ldots, f_n$ generate R as an R_0-algebra.*

Therefore, an $\mathbb{N}$-graded ring R is Noetherian if and only if R_0 is Noetherian and R is algebra-finite over R_0.

Proof. If $R = R_0[f_1, \dots, f_n]$, then any element $r \in R_+$ can be written as a polynomial expression $r = P(f_1, \dots, f_n)$ for some $P \in R_0[\underline{x}]$ with no constant term. Each monomial of P is a multiple of some x_i, and thus $r \in (f_1, \dots, f_n)$.

To show that $R_+ = (f_1, \dots, f_n)$ implies $R = R_0[f_1, \dots, f_n]$, it suffices to show that any homogeneous element $r \in R$ can be written as a polynomial expression in the f's with coefficients in R_0. We induce on the degree of r, with degree 0 as a trivial base case. For r homogeneous of positive degree, we must have $r \in R_+$, so by assumption we can write $r = a_1 f_1 + \cdots + a_n f_n$; moreover, since r and $f_1, \dots, f_n$ are all homogeneous, we can choose each coefficient a_i to be homogeneous of degree $|r| - |f_i|$. By the induction hypothesis, each a_i is a polynomial expression in the f's, so we are done.

For the final statement, if R_0 is Noetherian and R algebra-finite over R_0, then R is Noetherian by the Hilbert Basis Theorem. If R is Noetherian, then $R_0 \cong R/R_+$ is Noetherian. Moreover, R is algebra-finite over R_0 since R_+ is generated as an ideal by finitely many homogeneous elements by Noetherianity, so by the first statement, we get a finite algebra generating set for R over R_0. □

2.2. **Application: Finite generation rings of invariants.** If R is a graded ring, and G is a group acting on R by degree-preserving automorphisms, then R^G is a graded subring of R, meaning R^G is graded with respect to the same grading monoid.

Using this perspective, we can now give a different proof of the finite generation of invariant rings that works under different hypotheses. The proof we will discuss now is essentially Hilbert's proof. To do that, we need another notion that is very useful in commutative algebra.

Definition 2.15. Let S be an R-algebra corresponding to the ring homomorphism $\phi : R \to S$. We say that R is a *direct summand* of S if the map ϕ admits a left inverse as a map of R-modules.

Since the condition forces ϕ to be injective, we can assume it is an inclusion map (after renaming elements). Note that given any R-linear map $\pi : S \to R$, if $\pi(1) = 1$ then π is a splitting: indeed, $\pi(R) = \pi(r \cdot 1) = r\pi(1) = r$ for all $r \in R$.

Being a direct summand is really nice, since many good properties of S pass onto its direct summands.

Definition 2.16. Let $\phi : R \to S$ be a ring homomorphism.

- Given an ideal J in S, the preimage of J under ϕ is the *contraction* of J, denoted $\phi^{-1}(J)$ or $J \cap R$, even if ϕ is not an inclusion map.
- Given an ideal I in R, the *expansion* of I in S is the ideal of S generated by $\phi(I)$; we naturally denote this by IS .

Lemma 2.17. *Let R be a direct summand of S. Then, for any ideal $I \subseteq R$, we have $IS \cap R = I$.*

Proof. Let π be the corresponding splitting. Clearly, $I \subseteq IS \cap R$. Conversely, if $r \in IS \cap R$, we can write $r = s_1 f_1 + \cdots + s_t f_t$ for some $f_i \in I$, $s_i \in S$. Applying π, we have

$$r = \pi(r) = \pi\left(\sum_{i=1}^{t} s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i f_i\right) = \sum_{i=1}^{t} \pi\left(s_i\right) f_i \in I.$$ □

Proposition 2.18. *Let R be a direct summand of S. If S is Noetherian, then so is R.*

Proof. Let

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

be a chain of ideals in R. The chain of ideals in S

$$I_1S \subseteq I_2S \subseteq I_3S \subseteq \cdots$$

stabilizes, so there exist J, N such that $I_nR = J$ for $n \geqslant N$. Contracting to R, we get that $I_n = I_nS \cap R = J \cap R$ for $n \geqslant N$, so the original chain also stabilizes. □

Proposition 2.19. *Let K be a field, and R be a polynomial ring over K. Let G be a finite group acting by degree preserving K-algebra automorphisms on R. Assume that the characteristic of K does not divide $|G|$. Then R^G is a direct summand of R.*

Proof. We consider the map $\rho : R \to R^G$ given by

$$\rho(r) = \frac{1}{|G|} \sum_{g \in G} g \cdot r.$$

First, note that the image of this map lies in R^G, since acting by g just permutes the elements in the sum, so the sum itself remains the same. We claim that this map ρ is a splitting for the inclusion $R^G \subseteq R$. To see that, let $s \in R^G$ and $r \in R$. We have

$$\rho(sr) = \frac{1}{|G|} \sum_{g \in G} g \cdot (sr) = \frac{1}{|G|} \sum_{g \in G} (g \cdot s)(g \cdot r) = \frac{1}{|G|} \sum_{g \in G} s(g \cdot r) = s\frac{1}{|G|} \sum_{g \in G} (g \cdot r) = s\rho(r),$$

so ρ is R^G-linear, and for $s \in R^G$,

$$\rho(s) = \frac{1}{|G|} \sum_{g \in G} g \cdot s = s.$$ □

Theorem 2.20 (Hilbert's finiteness theorem for invariants)**.** *Let K be a field, and R be a polynomial ring over K. Let G be a group acting by degree preserving K-algebra automorphisms on R. Assume that G is finite and $|G|$ does not divide the characteristic of K, or more generally, that R^G is a direct summand of R. Then R^G is a finitely generated K-algebra.*

Proof. Since G acts by degree preserving K-algebra automorphisms, R^G is an $\mathbb{N}$-graded subring of R with $R_0 = K$. Since R^G is a direct summand of R, R^G is Noetherian by Proposition 2.18. By our characterization of Noetherian graded rings, R^G is finitely generated over $R_0 = K$. □

Remark 2.21. One important thing about this proof is that it applies to many infinite groups. In particular, for any *linearly reductive group*, including $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{C})$, and $(\mathbb{C}^\times)^n$, we can construct a splitting map ρ.

Lecture of February 4, 2022

3. Affine varieties

3.1. **Definition and examples of affine varieties.** Our next goal is to study solution sets of polynomial equations. Such solutions sets have a fancy name.

Definition 3.1. Let K be a field. We define *affine n-space* over K, denoted $\mathbb{A}^n_K$, to be the set of n-tuples over K:

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

Observe that any $f \in K[x_1, \ldots, x_n]$ can be considered as a function on $\mathbb{A}^n_K$, where $f(a_1, \ldots, a_n)$ is result of specializing x_i to a_i for each i.

Definition 3.2. For any subset $S \subseteq K[x_1, \ldots, x_n]$, we set

$$\mathcal{Z}(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}.$$

We call $\mathcal{Z}(S)$ the *zero set* of S. A *subvariety* of $\mathbb{A}^n_K$ is a set of the form $\mathcal{Z}(S)$. An *affine variety*, or just a *variety*, is a subvariety of $\mathbb{A}^n_K$ for some n.

Remark 3.3. Note that if $L \supseteq K$ is a larger field, any polynomial $f \in K[x_1, \ldots, x_n]$ is also an element of $L[x_1, \ldots, x_n]$, and we can evaluate it at any point in $\mathbb{A}^n_L$. Thus, we may write $\mathcal{Z}_K(S)$ or $\mathcal{Z}_L(S)$ the distinguish between the zero sets over different fields.

Example 3.4.

(1) For $K = \mathbb{R}$ and $n = 2$, $\mathcal{Z}(y^2 - x^2(x+1))$ 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.

(2) For $K = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(z - x^2 - y^2)$ is a paraboloid in $\mathbb{A}^3_{\mathbb{R}}$, real three space.

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

(4) For $K = \mathbb{R}$ and $n = 3$, $\mathcal{Z}(xy, xz)$ is a line and a plane that cross transversely.

(5) Over an arbitrary field K, a linear subspace of $\mathbb{A}^n_K = K^n$ is a subvariety: such a subset is defined by some linear equations.

(6) For $K = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2 + 1) = \varnothing$. Note that $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2 + 1) \neq \varnothing$, since it contains $(i, 0)$.

(7) For $K = \mathbb{R}$, $\mathcal{Z}_{\mathbb{R}}(x^2 + y^2) = \{(0,0)\}$. On the other hand, $\mathcal{Z}_{\mathbb{C}}(x^2 + y^2)$ is a union of two "lines" in $\mathbb{C}^2$ (or two planes, in the "real" sense), given by the equations $x + iy = 0$ and $x - iy = 0$.

(8) The subset $\mathbb{A}^2_K \backslash \{(0,0)\}$ is not an algebraic subset of $\mathbb{A}^2_K$ if K is infinite. Why?

(9) The graph of the sine function is not an algebraic subset of $\mathbb{A}^2_{\mathbb{R}}$. Why not?

(10) For $K = \mathbb{R}$ or $\mathbb{C}$, the set

$$X = \{(t, t^2, t^3) \mid t \in K\}$$

is an algebraic variety, though it isn't clear from this description. In fact, $X = \mathcal{Z}(y - x^2, z - x^3)$. To see the containment "$\subseteq$", for $(t, t^2, t^3) \in X$, we have $t^2 - t^2 = 0$ and $t^3 - t^3 = 0$. For the containment "$\supseteq$", let $(a, b, c) \in \mathcal{Z}(y - x^2, z - x^3)$, so $b = a^2$ and $c = a^3$. Setting $t = a$, we get that $(a, b, c) = (t, t^2, t^3) \in X$. The same argument works over $\mathbb{C}$.

(11) For $K = \mathbb{R}$ or $\mathbb{C}$, the set

$$X = \{(t^3, t^4, t^5) \mid t \in \mathbb{R}\}$$

is an algebraic variety, though again it needs justification. Consider $Y = \mathcal{Z}(y^3 - x^4, z^3 - x^5)$; clearly $X \subseteq Y$. Over $\mathbb{R}$, for $(a, b, c) \in Y$, take $t = \sqrt[3]{a}$; then $a = t^3$, $b^3 = a^4$ means $b = \sqrt[3]{a^4}$, so $b = t^4$, and similarly $c = t^5$, so $X = Y$. We were using uniqueness of cube roots in this argument though, so we need to reconsider over $\mathbb{C}$. Indeed, if ω is a cube root of unity, then $(1, 1, \omega) \in Y \smallsetminus X$, so we need to do better. Let's try $Z = \mathcal{Z}(y^3 - x^4, z^3 - x^5, z^4 - y^5)$. Again, $X \subseteq Z$. Say that $(a, b, c) \in \mathbb{A}^3_{\mathbb{C}}$ are in Z, and let s be a cube root of a. Then $b^3 = a^4 = (s^4)^3$ implies that $b = \omega s^4$ for some cube root of unity ω' (maybe 1, maybe not). Similarly $c^3 = a^4 = (s^5)^3$ implies that $c = \omega'' s^5$ for some cube root of unity ω'' (maybe 1, maybe ω', maybe not). So at least $(a, b, c) = (s^3, \omega' s^4, \omega'' s^5)$. Let $t = \omega' s$. Then $(s^3, \omega' s^4, \omega'' s^5) = (t^3, t^4, \omega s^5)$, where $\omega = (\omega')^2 \omega''$ is again some cube root of unity. The equation $b^5 = c^4$ shows that $t^2 0 = \omega^5 t^2 0$. If $t \neq 0$, this shows $\omega = 1$, so $(a, b, c) = (t^3, t^4, t^5)$; if $t = 0$, then $(a, b, c) = (0, 0, 0) = (0^3, 0^4, 0^5)$. Thus, $X = Z$.

(12) For any field K and elements $a_1, \ldots, a_d \in K$, we have

$$\mathcal{Z}(x_1 - a_1, \ldots, x_d - a_d) = \{(a_1, \ldots, a_d)\}.$$

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

(13) Here is an example from linear algebra. Fix a field K and consider the set of pairs (A, v) of 2×2 matrices and 2×1 vectors over K. We can again identify this with $\mathbb{A}^6_K$; let's call our variables $x_{11}, x_{12}, x_{21}, x_{22}, y_1, y_2$, where we are thinking of $A = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ and $v = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$. The set X of pairs (A, v) such that $Av = 0$ is a subvariety of $\mathbb{A}^6_K$:

$$X = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + x_{22}y_2).$$

(14) Let's take another linear algebra example. We can identify the set of 2×3 matrices over a field K with $\mathbb{A}^6_K$. To make this line up a little more naturally, let's label our variables as $x_{11}, x_{12}, x_{13}, x_{21}, x_{22}, x_{23}$. I claim that the set X of matrices of rank < 2 is a subvariety of $\mathbb{A}^6_K$. To see this, we need to find equations. For a 2×3 matrix A to have rank < 2, it is necessary and sufficient that each 2×2 submatrix have rank < 2, which is equivalent to each of the 2×2 minors (subdeterminants) of the matrix to be zero. Thus,

$$X = \mathcal{Z}(x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{23} - x_{13}x_{21}, x_{12}x_{23} - x_{13}x_{22}).$$

Proposition 3.5. *Let K be a field and $R = K[x_1, \ldots, x_n]$. Let $S, S_\lambda, T \subseteq R$ be arbitrary subsets, and $I, I_\lambda, J \subseteq R$ be ideals.*

(0) $\mathcal{Z}(1) = \varnothing$ *and* $\mathcal{Z}(0) = \mathbb{A}^n_K$.
(1) *If $S \subseteq T$, then $\mathcal{Z}(S) \supseteq \mathcal{Z}(T)$.*
(2) *If $I = (S)$ is the ideal generated by S, then $\mathcal{Z}(S) = \mathcal{Z}(I)$.*
(3) $\mathcal{Z}(\bigcup_{\lambda \in \Lambda} S_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{Z}(S_\lambda)$.
(3') $\mathcal{Z}(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{Z}(I_\lambda)$.
(4) $\mathcal{Z}(\{fg \mid f \in S, g \in T\}) = \mathcal{Z}(S) \cup \mathcal{Z}(T)$.
(4') $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

Proof. (0) is clear, since 1 is never equal to zero and 0 is always zero. (1) is also clear, since imposing more equations cannot enlarge the solution set.

For (2), we have $\mathcal{Z}(I) \subseteq \mathcal{Z}(S)$ by (1). On the other hand, if $f_1, \ldots, f_m \in S$ and $r_1, \ldots, r_m \in R$, and $(a_1, \ldots, a_n) \in \mathcal{Z}(S)$, then $f_i(a_1, \ldots, a_n) = 0$ for all i, so

$$(\sum_i r_i f_i)(a_1, \ldots, a_n) = \sum_i r_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) = 0,$$

so $(a_1, \ldots, a_n) \in \mathcal{Z}(\sum_i r_i f_i)$. Thus, $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$. That is, $\mathcal{Z}(S) \subseteq \mathcal{Z}(I)$. Similarly...

(3) is clear: for a point to satisfy be a solution to all of the equations in each set S_λ, it is equivalent to be a solution of each set of equations S_λ. For (3'), using (2) and (3), since $\sum_{\lambda \in \Lambda} I_\lambda$ is the ideal generated by $\bigcup_{\lambda \in \Lambda} I_\lambda$, we have

$$\mathcal{Z}(\sum_{\lambda \in \Lambda} I_\lambda) = \mathcal{Z}(\bigcup_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} \mathcal{Z}(I_\lambda).$$

For (4), it is clear that

$$\mathcal{Z}(S) \cup \mathcal{Z}(T) \subseteq \mathcal{Z}(\{fg \mid f \in S, g \in T\}),$$

since $f(a_1, \ldots, a_n) = 0$ for all $f \in S$ implies $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$ for all $f \in S$ and all $g \in T$. On the other hand, if $(a_1, \ldots, a_n) \notin \mathcal{Z}(S) \cup \mathcal{Z}(T)$, then there is some $f \in S$ and some $g \in T$ with $f(a_1, \ldots, a_n) \neq 0$ and $g(a_1, \ldots, a_n) \neq 0$, so $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) \neq 0$.

For (4'), since $IJ \subseteq I \cap J \subseteq I$ and $I \cap J \subseteq J$), by (1) we get

$$\mathcal{Z}(I) \cup \mathcal{Z}(J) \subseteq \mathcal{Z}(I \cap J) \subseteq \mathcal{Z}(IJ).$$

On the other hand, by (2) and (4) we get

$$\mathcal{Z}(IJ) \subseteq \mathcal{Z}(\{fg \mid f \in I, g \in J\}) = \mathcal{Z}(I) \cup \mathcal{Z}(J),$$

so the equalities hold throughout. □

Lecture of February 7, 2022

Remark 3.6. A basic corollary of (2) above and the Hilbert basis theorem says that every system of polynomial equations is equivalent to a finite one! Indeed, for any set S, $\mathcal{Z}(S) = \mathcal{Z}(I)$ for $I = (S)$, and since $K[x_1, \dots, x_n]$ is Noetherian, $S = (f_1, \dots, f_m)$ for some m, so $\mathcal{Z}(S) = \mathcal{Z}(f_1, \dots, f_m)$.

Definition 3.7. Let K be a field, and $X \subseteq \mathbb{A}^n_K$ be a subset. We define

$$\mathcal{I}(X) := \{f \in K[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}$$

One evident relation between the two notions: for a subset $X \subseteq \mathbb{A}^n_K$ and a subset $S \subseteq K[x_1, \dots, x_n]$, we have

$$X \subseteq \mathcal{Z}(S) \iff \text{each } s \in S \text{ vanishes at each } x \in X \iff S \subseteq \mathcal{I}(X).$$

Definition 3.8. The *radical* of an ideal I in a ring R is the ideal

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

An ideal is a *radical ideal* if $I = \sqrt{I}$.

To see that $\sqrt{I}$ is an ideal, note that if $f^m, g^n \in I$, then

$$\begin{aligned}(f+g)^{m+n-1} &= \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} f^i g^{m+n-1-i} \\ &= f^m \left(f^{n-1} + \binom{m+n-1}{1} f^{n-2} g + \cdots + \binom{m+n-1}{n-1} g^{n-1} \right) \\ &+ g^n \left(\binom{m+n-1}{n} f^{m-1} + \binom{m+n-1}{n+1} f^{m-2} g + \cdots + g^{m-1} \right) \in I,\end{aligned}$$

and $(rf)^m = r^m f^m \in I$.

Note that $I \subset R$ is radical if and only if R/I has a nonzero nilpotent elements; i.e., R/I is *reduced*.

Proposition 3.9. *Let K be a field, and X, X_λ, Y be subsets of $\mathbb{A}^n_K$.*

(0) *$\mathcal{I}(\varnothing) = R$ and, if K is infinite, $\mathcal{I}(\mathbb{A}^n_K) = 0$.*
(1) *If $X \subseteq Y$, then $\mathcal{I}(X) \supseteq \mathcal{I}(Y)$.*
(2) *$\mathcal{I}(X)$ is a radical ideal.*

Proof. For (0), it is clear that $\mathcal{I}(\varnothing) = R$. Assume K is infinite. We show by induction on n that a nonzero polynomial in $K[x_1, \dots, x_n]$ is nonzero at some point in $\mathbb{A}^n_K$. The case $n = 1$ is standard: a polynomial in $K[x]$ of degree d can have at most d roots. Now, let $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ be a nonzero polynomial. If f is a nonzero constant, it is nonzero at any point. Otherwise, we can assume that f nontrivially involves some variable, say x_n. Write

$$f(x_1, \dots, x_n) = f_d(x_1, \dots, x_{n-1}) x_n^d + \cdots + f_0(x_1, \dots, x_{n-1}).$$

If f is identically zero, then for every $(a_1, \ldots, a_{n-1}) \in \mathbb{A}_K^{n-1}$,

$$f_d(a_1, \ldots, a_{n-1})x_n^d + \cdots + f_0(a_1, \ldots, a_{n-1})$$

is a polynomial in one variable that is identically zero, so is the zero polynomial, so each $f_i(a_1, \ldots, a_{n-1})$ is identically zero. By the induction hypothesis, these are the zero polynomial, so $f(x_1, \ldots, x_n)$ is the zero polynomial, as required.

(1) is clear.

For (2), note that $f, g \in \mathcal{I}(X)$ and $r \in R$ implies $X \subseteq \mathcal{Z}(f, g)$ implies $X \subseteq \mathcal{Z}(rf+g)$ implies $rf+g \in \mathcal{I}(X)$, so $\mathcal{I}(X)$ is an ideal. If $f^t \in \mathcal{I}(X)$, then $f(a_1, \ldots, a_n)^t = 0$ for all $(a_1, \ldots, a_n) \in X$, so $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in X$, and $f \in \mathcal{I}(X)$. □

Determining $\mathcal{I}(X)$ can be very difficult; there was already some work involved in settling $\mathcal{I}(\mathbb{A}_K^n)$! We will explore the relationship between the associations $\mathcal{Z}$ and $\mathcal{I}$ more soon.

3.2. **Morphisms of varieties and coordinate rings.** The natural condition for a reasonable map between two varieties is that it should also be made from polynomials.

Definition 3.10. Suppose X is a subvariety of $\mathbb{A}_K^m$ and Y is a subvariety of $\mathbb{A}_K^n$. A *morphism of varieties* or *algebraic map* or *regular map* from X to Y is a function $\phi : X \to Y$ defined coordinatewise by polynomials $g_1, \ldots, g_n \in K[x_1, \ldots, x_m]$, that is

$$\phi(a_1, \ldots, a_m) = (g_1(a_1, \ldots, a_m), \ldots, g_n(a_1, \ldots, a_m)) \text{ for all } \underline{a} \in X.$$

Not every choice of $g_1, \ldots, g_n$ will give such a morphism, because the tuple $(g_1(\underline{a}), \ldots, g_n(\underline{a}))$ has to satisfy the equations of Y. Furthermore, different choices of $g_1, \ldots, g_n$ may yield the same morphism.

A morphism of varieties $\phi : X \to Y$ is an *isomorphism* if there is some $\phi : Y \to X$ such that $\phi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \phi = \mathrm{id}_X$.

Example 3.11.

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

(2) Take an infinite field, and let Y be the classical cuspidal curve:

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

Define

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

ϕ is an algebraic map from $\mathbb{A}_K^1$ 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. However, it is not an isomorphism. Indeed, if it were, we would have some map ψ such that $\psi \circ \phi = \mathrm{id}_{\mathbb{A}_K^1}$. This ψ would be given by a polynomial h in two variables such that $h(t^2, t^3) = t$. It is easy to see that no such h exists.

(3) Consider $\mathbb{A}_K^6$ as the space of 2×3 matrices over K with coordinates $x_{11}, \ldots, x_{23}$, and consider $\mathbb{A}_K^5$ as the space of pairs of 2×1 and 1×3 matrices over K with coordinates y_1, y_2, z_1, z_2, z_3. The map

of matrix multiplication from $\mathbb{A}^5_K$ to $\mathbb{A}^6_K$ is a regular map:

$$(y_1, y_2, z_1, z_2, z_3) \mapsto \begin{bmatrix} y_1z_1 & y_1z_2 & y_1z_3 \\ y_2z_1 & y_2z_2 & y_2z_3 \end{bmatrix}.$$

Definition 3.12. 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

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

Recall that $\mathcal{I}(X)$ is a radical ideal, and so $K[X]$ is necessarily a reduced, finitely generated K-algebra. An algebra A is *reduced* if $a^n = 0$ implies $a = 0$ in A.

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

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

Remark 3.13. Let $Y = \mathbb{A}^1_K$ and let X be any algebraic subset of $\mathbb{A}^n_K$ for some n. Then an algebraic map $\phi : X \to \mathbb{A}^1_K$ is determined by a polynomial $f \in K[x_1, \ldots, x_n]$. Two such polynomials f, g give the same map G if they agree on X, that is if $f - g \in \mathcal{I}(X)$. So, we have a bijection of sets

$$K[X] \cong \{\text{algebraic morphisms from } X \text{ to } \mathbb{A}^1_K\}.$$

In this way, $K[X]$ is analogous to the ring

$$\mathcal{C}_{\mathbb{R}}(T) := \{\text{the collection of continuous real valued functions on } T\}.$$

Definition 3.14. Let K be a field. Let $X \subseteq \mathbb{A}^m_K$ and $Y \subseteq \mathbb{A}^n_K$ be affine varieties. Let $\phi : X \to Y$ be a morphism given by $(g_1(x), \ldots, g_n(x))$, with $g_i \in K[x_1, \ldots, x_m]$. We define

$$\begin{array}{ccc} K[Y] & \xrightarrow{\quad\phi^*\quad} & K[X] \\ f(y_1, \ldots, y_n) & \longmapsto & f(g_1(x), \ldots, g_n(x)) \end{array}$$

Alternatively, thinking of $f \in K[Y]$ as a regular map from $Y \to A^1_K$, we have

$$\begin{array}{ccc} K[Y] & \xrightarrow{\quad\phi^*\quad} & K[X] \\ Y \xrightarrow{f} \mathbb{A}^1_K & \rightsquigarrow & X \xrightarrow{f\phi} \mathbb{A}^1_K \\ & & \| \\ & & X \xrightarrow{\phi} Y \xrightarrow{f} \mathbb{A}^1_K \end{array}$$

We may call this the *homomorphism induced by ϕ* or the *pullback* of ϕ.

Optional Exercise 3.15. Show that the rule ϕ^* is a well-defined ring homomorphism, and that the map $\phi \mapsto \phi^*$ is well-defined.

Optional Exercise 3.16. For any field K, there is a contravariant functor from affine varieties over K to affine K-algebras that

- on objects, maps a variety X to its coordinate ring $K[X]$,
- on morphisms, maps a morphism of varieties $X \xrightarrow{\phi} Y$ to its pullback $K[Y] \xrightarrow{\phi^*} K[X]$.

Proposition 3.17. *Let $X \subseteq \mathbb{A}^m_K$ and $Y \subseteq \mathbb{A}^n_K$ be affine varieties, and $\phi : X \to Y$ be a morphism. Then* $\ker(\phi^*) = \mathcal{I}(\operatorname{im}\phi)K[Y]$.

The proof is left as an exercise.

Lecture of February 9, 2022

3.3. The Zariski topology and irreducible varieties.

Definition 3.18. Let K be a field. The collection of subvarieties $X \subseteq \mathbb{A}^n_K$ is the collection of closed subsets in a topology on $\mathbb{A}^n_K$:

- $\varnothing = \mathcal{Z}(1)$ and $\mathbb{A}^n_K = \mathcal{Z}(0)$ are subvarieties,
- unions of two subvarieties are subvarieties (products of the equations), and
- arbitrary intersections of subvarieties are subvarieties (union of the equation sets).

This is called the *Zariski topology* on $\mathbb{A}^n_K$. Any subvariety of $\mathbb{A}^n_K$ obtains a *Zariski topology* as the subspace topology from $\mathbb{A}^n_K$.

This topology is not very similar to the Euclidean topology on a manifold; it is much coarser.

Example 3.19. Let K be an infinite field. The closed subsets in the Zariski topology on $\mathbb{A}^1_K$ are just the finite subsets, along with the whole space. Note that this topology is not Hausdorff; quite on the contrary, any two nonempty open sets have infinite intersection!

Here is a nice use of the topological structure.

Proposition 3.20. *Let $X \subseteq \mathbb{A}^n_K$ be a subset. Then $\mathcal{Z}(\mathcal{I}(X)) = \overline{X}$, the closure of X in the Zariski topology.*

Proof. Clearly $X \subseteq \mathcal{Z}(\mathcal{I}(X))$ and $\mathcal{Z}(\mathcal{I}(X))$ is closed, so $\overline{X} \subseteq \mathcal{Z}(\mathcal{I}(X))$. On the other hand, $\overline{X} = \bigcap_{\substack{W \supseteq X \\ W \text{ closed}}} W$. For $W \supseteq X$ closed, write $W = \mathcal{Z}(J)$; then $J \subseteq \mathcal{I}(W)$ and $W \supseteq X$ implies $\mathcal{I}(W) \subseteq \mathcal{I}(X)$, so $J \subseteq \mathcal{I}(X)$, hence $\mathcal{Z}(\mathcal{I}(X)) \subseteq \mathcal{Z}(J) = W$. It follows that $\mathcal{Z}(\mathcal{I}(X)) \subseteq \overline{X}$ as well. □

Remark 3.21. Note as a consequence that the function

$$\{\text{subvarieties of } \mathbb{A}^n_K\} \xrightarrow{\mathcal{I}} \{\text{ideals of } K[x_1, \ldots, x_n]\}$$

is injective, since $\mathcal{Z}$ serves as a left inverse.

Recall that a topological space is connected if it cannot be written as the disjoint union of two closed subsets. Here is a much stronger notion of a similar flavor.

Definition 3.22. A topological space is *irreducible* if it cannot be written as a union of two proper closed subsets.

This is much stronger than connected, since there is no disjointness condition on the sets.

Optional Exercise 3.23.
(1) If $Y \subseteq X$ is irreducible, then so is $\overline{Y} \subseteq X$.
(2) If X is an irreducible topological space, and $f : X \to Y$ is continuous, then $f(X)$ is irreducible.
(3) Any nested union $\bigcup_{\lambda \in \Lambda} X_\lambda$ (for a totally ordered set Λ and $X_\mu \subseteq X_\nu$ for $\mu \leqslant \nu$) of irreducible spaces is irreducible.

Optional Exercise 3.24. A topological space is Hausdorff if and only if every irreducible subset is a point.

Proposition 3.25. *Let K be an infinite field. Affine space $\mathbb{A}^n_K$ is irreducible.*

Proof. Say that $\mathbb{A}^n_K = \mathcal{Z}(I) \cup \mathcal{Z}(J)$ for some ideals I, J. We need to show either $\mathcal{Z}(I) = \mathbb{A}^n_K$ or $\mathcal{Z}(J) = \mathbb{A}^n_K$. Note that $\mathbb{A}^n_K = \mathcal{Z}(IJ)$. We must have $IJ = 0$: if $f \in IJ \smallsetminus 0$, then $\mathcal{Z}(IJ) \subseteq \mathcal{Z}(f) \subsetneq \mathbb{A}^n_K$ since $\mathcal{I}(\mathbb{A}^n_K) = 0$. If I and J are both nonzero, take $f \in I \smallsetminus 0$, and $g \in J \smallsetminus 0$; we get $fg \in IJ \smallsetminus 0$, which is a contradiction. Thus, without loss of generality, $I = 0$, so $\mathcal{Z}(I) = \mathbb{A}^n_K$. □

Example 3.26. Affine space over a finite field is reducible: points are subvarieties, so finite unions of points are, and hence

$$\mathbb{A}^n_K = \{(0, \dots, 0)\} \cup \mathbb{A}^n_K \smallsetminus \{(0, \dots, 0)\}$$

is a decomposition into proper subvarieties.

Example 3.27. The variety $\mathcal{Z}_{\mathbb{R}}(xy, xz)$ is reducible: it is $\mathcal{Z}_{\mathbb{R}}(x) \cup \mathcal{Z}_{\mathbb{R}}(y, z)$, the union of a line and a plane, which are varieties.

Example 3.28. Let K be an infinite field. Think of $\mathbb{A}^6_K$ as the set of pairs of 2×2 matrices A (with coordinates x_{ij}) and 2×1 vectors v (with coordinates y_1, y_2), and let $X = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2)$ be the variety of pairs such that $Av = 0$. If $Av = 0$ then either $v = 0$, or else v is a nonzero vector in the kernel of A, so $\det(A) = 0$. Thus, $X = X_1 \cup X_2$, where

$$X_1 = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2, y_1, y_2) = \mathcal{Z}(y_1, y_2)$$

$$X_2 = \mathcal{Z}(x_{11}y_1 + x_{12}y_2, x_{21}y_1 + y_{22}y_2, x_{11}x_{22} - x_{12}x_{21}),$$

so X is reducible.

Lecture of February 11, 2022

Example 3.29. Let K be an infinite field. Think of $\mathbb{A}^6_K$ as the set of 2×3 matrices (with coordinates x_{ij}), and let X be the variety of matrices of rank at most 1. Any matrix $A \in X$ of rank at most one can be written as $A = BC$ for some 2×1 matrix B and some 1×3 matrix C, and conversely any such product has rank at most 1. It follows that X is the image of the morphism

$$\mathbb{A}^5 \longrightarrow \mathbb{A}^6$$

$$(y_1, y_2, z_1, z_2, z_3) \longmapsto \begin{pmatrix} y_1z_1 & y_1z_2 & y_1z_3 \\ y_2z_1 & y_2z_2 & y_2z_3 \end{pmatrix}$$

and hence is irreducible.

Definition 3.30. Let X be a topological space. We say that X is a *Noetherian* topological space if the poset of open sets under containment has ACC, or equivalently that the poset of closed subsets has DCC.

Lemma 3.31. *Any affine variety X is a Noetherian topological space with the Zariski topology.*

Proof. It suffices to deal with $\mathbb{A}^n_K$, since subspaces of Noetherian spaces are Noetherian. If there was an infinite descending chain of closed subvarieties of $\mathbb{A}^n_K$, applying $\mathcal{I}$, we would obtain an infinite ascending chain of ideals in $K[x_1, \dots, x_n]$, which contradicts Hilbert's Basis Theorem. □

Definition 3.32. Let X be a topological space. A maximal irreducible subspace of X is called an *irreducible component* of X.

Remark 3.33. An irreducible component of a space is closed, since the closure of an irreducible subset is closed.

Proposition 3.34. *Let X be a topological space.*

(1) *X is the union of its irreducible components.*
(2) *If $X = X_1 \cup \cdots \cup X_n$ with each X_i irreducible, and suppose that $X_i \nsubseteq \bigcup_{j \neq i} X_j$; i.e., the union $X = X_1 \cup \cdots \cup X_n$ is* irredundant*. Then $\{X_1, \ldots, X_n\}$ is the collection of irreducible components of X.*
(3) *If X is Noetherian, then X has finitely many irreducible components. Hence, if X is Noetherian, it can be written as an irredundant finite union of irreducible components in a unique way.*

Proof. (1) It suffices to show that any point is in an irreducible component. Let $x \in X$, and consider the collection of irreducible subsets of X that contain x. This is nonempty, since $\{x\}$ is in the collection. By the exercise above, the union of any chain under inclusion is again irreducible, so Zorn's lemma applies. Such a subset must be a maximal irreducible subset, since any larger subset also contains x.

(2) Let Y be an irreducible component of X. Then $Y = (X_1 \cap Y) \cup \cdots \cup (X_n \cap Y)$ implies that $X_i \cap Y = Y$, so $Y \subseteq X_i$ for some i. By maximality, we must have $Y = X_i$. This shows that every irreducible component is on the list.

Conversely, for some X_i, take $Y \supseteq X_i$ to be an irreducible component: we can do this by the same Zorn's Lemma argument as in the previous part. By what we just showed, $Y = X_j$ for some j. By irredundancy, we must have $i = j$, so X_i is an irreducible component.

(3) Consider the collection of closed subsets of X that are not finite unions of irreducibles. If this collection is nonempty (in particular, if X is not a finite union of irreducibles), it has a minimal element by DCC; call it Z. In particular, Z is reducible, so write $Z = Z' \cup Z''$ with Z', Z'' closed proper subsets of Z. Since they are smaller than Z, they are finite unions of irreducibles. Putting them together expresses Z as a finite union of irreducibles. □

3.4. **Prime and maximal ideals.**

Theorem 3.35. *Let K be a field, and $X \subseteq \mathbb{A}^n_K$ be an affine variety.*

(1) *X is irreducible if and only if $\mathcal{I}(X)$ is a prime ideal.*
(2) *X is a point if and only if $\mathcal{I}(X)$ is a maximal ideal.*

Proof. (1) First we show that if $\mathcal{I}(X)$ is not prime, then X is reducible. Suppose that $f, g \notin \mathcal{I}(X)$ and $fg \in \mathcal{I}(X)$. Since $f \notin \mathcal{I}(X)$, f does not vanish at some point of X, so $X \nsubseteq \mathcal{Z}(f)$. Thus,

$$\mathcal{Z}(\mathcal{I}(X) + (f)) = \mathcal{Z}(\mathcal{I}(X)) \cap \mathcal{Z}(f) = X \cap \mathcal{Z}(f) \subsetneq X,$$

and likewise $\mathcal{Z}(\mathcal{I}(X) + (g)) \subsetneq X$. But

$$X \supseteq \mathcal{Z}(\mathcal{I}(X)+(f)) \cup \mathcal{Z}(\mathcal{I}(X)+(g)) = \mathcal{Z}((\mathcal{I}(X)+(f))(\mathcal{I}(X)+(g))) = \mathcal{Z}(\mathcal{I}(X)^2+(f,g)\mathcal{I}(X)+(fg)) \supseteq \mathcal{Z}(\mathcal{I}(X)) = X,$$

so $\mathcal{Z}(\mathcal{I}(X) + (f)) \cup \mathcal{Z}(\mathcal{I}(X) + (g)) = X$. This shows that X is reducible.

Now, we show that if X is reducible, then $\mathcal{I}(X)$ is not prime. Write $X = Y \cup Z$ with Y, Z closed and $Y, Z \subsetneq X$. We must that $\mathcal{I}(X) \subsetneq \mathcal{I}(Y), \mathcal{I}(Z)$, and $\mathcal{I}(Y) \neq \mathcal{I}(Z)$, since $Y \neq Z$. Take $f \in \mathcal{I}(Y) \smallsetminus \mathcal{I}(Z)$ and $g \in \mathcal{I}(Z) \smallsetminus \mathcal{I}(Y)$. Then $fg \in \mathcal{I}(Y) \cap \mathcal{I}(Z)$, so

$$\mathcal{Z}(fg) \supseteq \mathcal{Z}(\mathcal{I}(Y) \cap \mathcal{I}(Z)) = Y \cup Z = X.$$

Thus, $fg \in \mathcal{I}(X)$. This shows that $\mathcal{I}(X)$ is not prime.

(2) First, take $X = \{(a_1 \dots, a_n)\}$. We have $x_i - a_i \in \mathcal{I}(X)$ for all i, so $\mathfrak{m} := (x_1 - a_1, \dots, x_n - a_n) \subseteq \mathcal{I}(X)$. The ideal $\mathfrak{m}$ is maximal, since the quotient $K[x_1, \dots, x_n]/\mathfrak{m} \cong K$ is a field. Since the only larger ideal is the full ring itself, and $1 \notin \mathcal{I}(X)$, we must have $\mathcal{I}(X) = \mathfrak{m}$ is maximal.

On the other hand, if $X \supsetneq \{(a_1 \dots, a_n)\}$, then $\mathcal{I}(X) \subsetneq \mathcal{I}(\{(a_1 \dots, a_n)\})$, so $\mathcal{I}(X)$ is not maximal. □

Corollary 3.36. *Let K be a field.*

(1) *The maps $\mathcal{Z}$ and $\mathcal{I}$ induce a bijection*

$$\{\text{maximal ideals } \mathfrak{m} \text{ of } R = K[x_1, \dots, x_n] \text{ such that } R/\mathfrak{m} \cong K\} \leftrightarrow \mathbb{A}^n_K$$

(2) *For any affine variety X, there is a bijection*

$$\{\text{maximal ideals } \mathfrak{m} \text{ of } K[X] \text{ such that } K[X]/\mathfrak{m} \cong K\} \leftrightarrow X$$

Lecture of February 14, 2022

Proof. For (1), we need to see that $\xrightarrow{\mathcal{Z}}$ and $\xleftarrow{\mathcal{I}}$ restrict to maps to/from the prescribed source and target. For $\mathcal{Z}$, let $\mathfrak{m}$ be a maximal ideal with residue field K, and consider $\pi : R \to R/\mathfrak{m} \cong K$. We then have that $\pi(x_i) = a_i$ for some $a_i \in K$, so $(x_1 - a_1, \dots, x_n - a_n) \subseteq \ker(\pi) = \mathfrak{m}$, and this ideal is maximal, so equality holds. Then $\mathcal{Z}(\mathfrak{m}) = \{(a_1, \dots, a_n)\}$, so $\mathcal{Z}$ gives a well-defined map from left to right. On the other hand, from the last theorem, we see that for any point, $\mathcal{I}$ yields an ideal of this form so $\mathcal{I}$ restricts to a well-defined map here. We know that $\mathcal{Z}(\mathcal{I}(x)) = x$ for a point x since a point is closed, and for an ideal $\mathfrak{m}$ as above, $\mathcal{I}(\mathcal{Z}(\mathfrak{m}))$ is a maximal ideal containing $\mathfrak{m}$, so must equal $\mathfrak{m}$.

For (2), we note that there is a bijection between maximal ideals of $K[X]$ and maximal ideals of $K[x_1, \dots, x_n]$ that contain $\mathcal{I}(X)$; moreover $\mathcal{I}(X) \subseteq \mathfrak{m}$ if and only if $\mathcal{Z}(\mathfrak{m}) \in \mathcal{Z}(\mathcal{I}(X)) = X$. Thus, the bijection from (1) induces a bijection between maximal ideals of $K[X]$ and points of X. □

To recap, over an any field K, the maps $\xleftarrow{\mathcal{Z}}$ and $\xrightarrow{\mathcal{I}}$ yield order-reversing maps between the collections below and satisfy $\mathcal{Z} \circ \mathcal{I} = \mathrm{id}$ in each case, so they induce bijections between the RHS and a subset of the LHS (the image of $\mathcal{I}$):

$$\begin{array}{cc} \underline{\text{in } K[x_1, \dots, x_n]} & \underline{\text{in } \mathbb{A}^n_K} \\ \{\text{radical ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{varieties}\} \\ \{\text{prime ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{irred vars}\} \\ \{\text{maximal ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} \{\text{points}\}. \end{array}$$

Likewise, for any variety X, we have order-reversing maps that induce bijections between the RHS and a subset of the LHS:

$$\begin{array}{cc} \underline{\text{in } K[X]} & \underline{\text{in } X} \\ \{\text{radical ideals}\} \leftrightarrows \{\text{subvarieties}\} \\ \{\text{prime ideals}\} \leftrightarrows \{\text{irred subvars}\} \\ \{\text{maximal ideals}\} \leftrightarrows \{\text{points}\}. \end{array}$$

In both cases, we identified the image of the last $\leftarrow$ as maximal ideals whose residue field was no bigger than the ground field.

Example 3.37. (1) The radical ideal $(0) \subseteq \mathbb{F}_p[x]$ is not in the image of $\mathcal{I}$ (i.e., is left of the the bijection above) over $K = \mathbb{F}_p$. Indeed, $\mathcal{I}(\mathcal{Z}(0)) = \mathcal{I}(\mathbb{A}^1_{\mathbb{F}_p}) = (x^p - x)$.

(2) The prime ideal $(x^2+y^2+z^2) \subseteq \mathbb{R}[x,y,z]$ is not in the image of $\mathcal{I}$ over $K = \mathbb{R}$: $\mathcal{I}(\mathcal{Z}(x^2+y^2+z^2)) = \mathcal{I}(\{(0,0,0\}) = (x,y,z)$.

(3) The maximal ideal $(x^2+1) \subseteq \mathbb{R}[x]$ is not in the image of $\mathcal{I}$ over $K = \mathbb{R}$: $\mathcal{I}(\mathcal{Z}(x^2+1)) = \mathcal{I}(\varnothing) = (1)$.

4. The Nullstellensatz and the prime spectrum

4.1. **Review of transcendence bases.**

Definition 4.1. 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 4.2. (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.

Lemma 4.3. *Let $\{x_1,\dots,x_m\}$ and $\{y_1,\dots,y_n\}$ be two transcendence bases for L over K. Then, there is some i such that $\{x_i, y_2,\dots,y_n\}$ is a transcendence basis.*

Proof. Since L is algebraic over $K(y_1,\dots,y_n)$, for each i there is some $p_i(t) \in K(y_1,\dots,y_n)[t]$ such that $p_i(x_i) = 0$. We can clear denominators to assume without loss of generality that $p_i(x_i) \in K[y_1,\dots,y_n][t]$.

We claim that there is some i such that $p_i(t) \notin K[y_2,\dots,y_n][t]$. If not, so $p_i(t) \in K[y_2,\dots,y_n][t]$ for all i, note that each x_i is algebraic over $K(y_2,\dots,y_n)$. Thus, $K(x_1,\dots,x_m)$ is algebraic over $K(y_2,\dots,y_n)$, and since L is algebraic over $K(x_1,\dots,x_m)$, y is algebraic over $K(y_2,\dots,y_n)$, which contradicts that $\{y_1,\dots,y_n\}$ is a transcendence basis. This shows the claim.

Now, we claim that for such i, $\{x_i,y_2,\dots,y_n\}$ is a transcendence basis. Thinking of the equation $p_i(x_i) = 0$ as a polynomial expression in $K[x_i,y_2,\dots,y_n][y_1]$, y_1 is algebraic over $K(x_i,y_2,\dots,y_n)$, hence $K(y_1,\dots,y_n)$ is algebraic over $K(x_i,y_2,\dots,y_n)$, and L as well.

If $\{x_i,y_2,\dots,y_n\}$ were algebraically dependent, take a polynomial equation $p(x_i,y_2,\dots,y_n) = 0$. Note that this equation must involve x_i, since $y_2,\dots,y_n$ are algebraically independent. We would then have $K(x_i,y_2,\dots,y_n)$ is algebraic over $K(y_2,\dots,y_n)$. But since y_1 is algebraic over $K(x_i,y_2,\dots,y_n)$, we would have that $K(y_1,\dots,y_n)$ is algebraic over $K(y_2,\dots,y_n)$, which would contradict that $y_1,\dots,y_n$ is a transcendence basis. □

Proposition 4.4. *If $\{x_1, \dots, x_m\}$ and $\{y_1, \dots, y_n\}$ are two transcendence bases for L over K, then $m = n$.*

Proof. Say that $m \leqslant n$. If the intersection has $s < m$ elements, then without loss of generality $y_1 \notin \{x_1, \dots, x_m\}$. Then, for some i, $\{x_i, y_2 \dots, y_n\}$ is a transcendence basis, and $\{x_1, \dots, x_m\} \cap \{x_i, y_2 \dots, y_n\}$ has $s + 1$ elements. Replacing $\{y_1, \dots, y_n\}$ with $\{x_i, y_2 \dots, y_n\}$ and repeating this process, we obtain a transcendence basis with n elements such that $\{x_1, \dots, x_m\} \subseteq \{y_1, \dots, y_n\}$. But we must then have that these two transcendence bases are equal, so $m = n$. □

4.2. **Nullstellensatz.**

Theorem 4.5 (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 $L = K[h_1, \dots, h_d]$. Since in particular $h_1, \dots, h_d$ 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 $h_1, \dots, h_c = x_1, \dots, x_c$ form a transcendence basis, and $h_{c+1}, \dots, h_d$ are algebraic over $K' = K(x_1, \dots, x_c)$. 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 $K[x_1, \dots, x_c]$ such that $K' = K[\frac{f_1}{g_1}, \dots, \frac{f_m}{g_m}]$. This implies that any element of K' can be written as a fraction with denominator $(g_1 \cdots g_m)^n$ for some n. The element $\frac{1}{g_1 \cdots g_m + 1} \in K'$ cannot be written this way; if so, we would have

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

for some v with $g_1 \cdots g_m \nmid v$ (since the polynomial ring is a UFD). But, the equation $g_1 \cdots g_m v + v = (g_1 \cdots g_m)^n$ contradicts this.

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

Lecture of February 16, 2022

Theorem 4.6 (Hilbert's Nullstellensatz (Weak Form))**.** *Let K be an algebraically closed field and J be an ideal of $K[x_1, \dots x_n]$. We have*

$$\mathcal{Z}(J) = \varnothing \text{ if and only if } J = K[x_1, \dots, x_n].$$

Remark 4.7. One direction is clear. The nontrivial direction, in its most basic form, says the following: Suppose we are given a system of polynomial equations

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

in n variables with coefficients in some algebraically closed field K. If the system has no solutions over K, then for some polynomials $g_1, \dots, g_m$ we have $\sum_i g_i f_i = 1$. One can think of $g_1, \dots, g_m$ as forming a "certificate" that there is no solution.

Proof. If $J = K[x_1, \dots, x_n]$, then $Z(J) = \varnothing$ since $1 = 0$ has no solutions.

We show that if $J \subset K[x_1, \ldots, x_n]$ is a proper ideal, then $Z(J) \neq \varnothing$. Since J is proper, it is contained in some maximal ideal $\mathfrak{m}$. By Zariski's Lemma, $K[x_1, \ldots, x_n]/\mathfrak{m} \cong K$, so we have $\mathcal{Z}(\mathfrak{m}) \neq \varnothing$. □

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

Remark 4.8 (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 4.9 (Hilbert's Nullstellensatz (Strong Form))**.** *Let K be an algebraically closed field and let J be an ideal in the polynomial ring $R = K[x_1, \ldots, x_n]$. Then, for $f \in R$, $\mathcal{Z}(f) \supseteq \mathcal{Z}(J)$ if and only if $f \in \sqrt{J}$.*

In particular, $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$.

Proof. The equations in $\sqrt{J}$ vanish on $\mathcal{Z}(J)$, so $\sqrt{J} \subseteq \mathcal{I}(\mathcal{Z}(J))$.

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

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

we see that it has no solution since $f(\underline{x}) = 0$ is a consequence of the first m equations. By the remark above, this implies that $\mathcal{Z}(JS + (yf - 1)) = \varnothing$, where $JS + (yf - 1)$ is an ideal in the polynomial ring $S = K[x_1, \ldots, x_n, y]$. 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 $S \to \mathrm{Frac}(R)$ 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). □

Corollary 4.10. *Let K be an algebraically closed field. The associations $\mathcal{Z}$ and $\mathcal{I}$ induce order-reversing bijections*

$$\begin{array}{cc} \underline{\text{in } K[x_1, \ldots, x_n]} & \underline{\text{in } \mathbb{A}^n_K} \\ \{\text{radical ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{varieties}\} \\ \{\text{prime ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{irred vars}\} \\ \{\text{maximal ideals}\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\leftrightarrows}} & \{\text{points}\}. \end{array}$$

In particular, given ideals I and J, we have $\mathcal{Z}(I) = \mathcal{Z}(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Likewise, for any variety X over an algebraically closed field, we have order-reversing bijections

$$\begin{array}{ccc} \underline{\textit{in } K[X]} & & \underline{\textit{in } X} \\ \{\textit{radical ideals}\} & \rightleftarrows & \{\textit{subvarieties}\} \\ \{\textit{prime ideals}\} & \rightleftarrows & \{\textit{irred subs}\} \\ \{\textit{maximal ideals}\} & \rightleftarrows & \{\textit{points}\}. \end{array}$$

Example 4.11. Recall that

$$X := \{(t^3, t^4, t^5) \mid t \in \mathbb{C}\} = \mathcal{Z}(I), \text{ where } I = (y^3 - x^4, z^3 - x^5, z^4 - y^5).$$

By the Nullstellensatz, $\mathcal{I}(X) = \sqrt{I}$. The ideal I is not radical: note that

$$x^9yz \equiv (x^4)(x^5)yz \equiv y^4z^4 \equiv y^9 \equiv x^{12} \equiv x^3y^3z^3 \qquad \mod I$$

and

$$x^6y^2z^2 \equiv x^2y^5z^2 \equiv x^2z^6 \equiv x^{12} \qquad \mod I$$

so

$$(x^3 - yz)^4 = x^{12} - 4x^9yz + 6x^6y^2z^2 - 4x^3y^3z^3 + y^4z^4 \equiv x^{12}(1 - 4 + 6 - 4 + 1) \equiv 0 \qquad \mod I.$$

One can show that $\sqrt{I} = (x^3 - yz, y^2 - xz, z^2 - x^2y)$.

4.3. **Spectrum of a ring.** As a consequence of the Nullstellensatz, for an algebraically closed field K and an algebra of the form $R = K[x_1, \ldots, x_n]/I$ that is reduced, we know that $I = \mathcal{I}(X)$ for some variety $X \subseteq \mathbb{A}^n_K$, and $R = K[X]$. We can recover X (as a set) from the ring R by taking the maximal ideals of R. Moreover, we can recover the Zariski topology on X: a subvariety of X corresponds to a (radical) ideal of R, so the closed subsets correspond to the sets of maximal ideals that contain a particular (radical) ideal of R. Moreover, we can reconstruct morphisms of varieties from the maps on their coordinate rings:

Optional Exercise 4.12. Let X, Y be affine varieties over an algebraically closed field with $R = K[X]$ and $S = K[Y]$. Let $\phi : X \to Y$ be an algebraic morphism, and $\phi^* : S \to R$ be the induced map on coordinate rings. Then the following diagram commutes:

$$\begin{array}{ccc} \operatorname{Max}(R) & \longrightarrow & \operatorname{Max}(S) \\ \downarrow & \mathfrak{m} \longmapsto (\phi^*)^{-1}(\mathfrak{m}) & \downarrow \\ X & \xrightarrow{\quad\phi\quad} & Y \end{array}$$

where the vertical maps send a maximal ideal of the form $(x_1 - a_1, \ldots, x_n - a_n)$ to the point $(a_1, \ldots, a_n)$; this is essentially the map $\mathcal{Z}$ on maximal ideals.

Remark 4.13. Loosely speaking, this exercise says that $\operatorname{Max}(-)$ can be thought of as a contravariant functor that, on the category of reduced finitely generated algebras over algebraically closed fields, is an inverse to the coordinate ring functor up to natural isomorphism. The precise statement is that functor yields an equivalence of categories.

Lecture of February 18, 2022

We now use a similar idea to construct a geometric object for every ring. However, we want this to be functorial, and in general the preimage of a maximal ideal is not maximal, e.g., for the inclusion $\mathbb{Z} \subseteq \mathbb{Q}$, (0) is maximal in $\mathbb{Q}$, but its contraction is (0) in $\mathbb{Z}$, which is not maximal. However, the preimage of a prime ideal is prime.

Lemma 4.14. *Let $R \to S$ be a ring homomorphism and $\mathfrak{p} \subset S$ be prime. Then $\mathfrak{p} \cap R$ is also prime.*

Definition 4.15. Let R be a ring. The *prime spectrum* of R, $\operatorname{Spec}(R)$, is the set of prime ideals of R.

Definition 4.16. For a ring R and an ideal I, we set

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

Proposition 4.17. *Let R be a ring, and I_λ, J be ideals (possibly improper).*

(0) *$V(R) = \varnothing$ and $V(0) = \operatorname{Spec}(R)$.*
(1) *If $I \subseteq J$, then $V(J) \subseteq V(I)$.*
(2) *$V(I) \cup V(J) = V(I \cap J) = V(IJ)$.*
(3) *$\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.*
(4) *$V(I) = V\sqrt{I}$*

Proof. We only deal with (2), as the others are straightforward. To see $V(I) \cup V(J) \subseteq V(I \cap J)$, just observe that if $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$, then $\mathfrak{p} \supseteq I \cap J$. Since $IJ \subseteq I \cap J$, we have $V(I \cap J) \subseteq V(IJ)$. To show $V(IJ) \subseteq V(I) \cup V(J)$, if $\mathfrak{p} \not\supseteq I, J$, let $f \in I \smallsetminus \mathfrak{p}$, and $g \in J \smallsetminus \mathfrak{p}$. Then $fg \in IJ \smallsetminus \mathfrak{p}$ since $\mathfrak{p}$ is prime. □

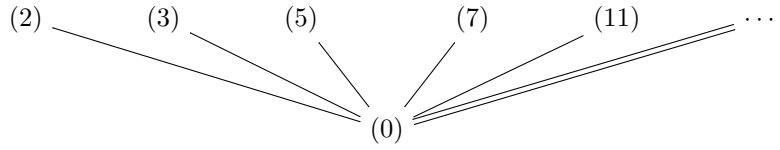
Definition 4.18. It follows that $\operatorname{Spec}(R)$ obtains a topology by setting the closed sets to be all sets of the form $V(I)$; this is the *Zariski topology* on $\operatorname{Spec}(R)$.

Optional Exercise 4.19. Note that $\operatorname{Spec}(R)$ is also a poset under inclusion. Show that the poset structure of $\operatorname{Spec}(R)$ can be recovered from the topology as follows:

$$\mathfrak{p} \subseteq \mathfrak{q} \quad \Leftrightarrow \quad \mathfrak{q} \in \overline{\{\mathfrak{p}\}}.$$

Example 4.20. For any affine variety X over an algebraically closed field, the spectrum of $K[X]$ consists of maximal ideals and nonmaximal primes. The maximal ideals are in bijection with the points of X; the other primes correspond to irreducible subvarieties of X. Thus, we can think of $\operatorname{Spec}(K[X])$ as X with "fake points" added in for each irreducible subvariety.

Example 4.21. The spectrum of $\mathbb{Z}$ is, as a poset:



The closed sets are of the form $V((n))$, which are the whole space when $n = 0$, the empty set with $n = 1$, and any finite union of things in the top row.

Definition 4.22 (Induced map on Spec)**.** Given a homomorphism of rings $\varphi : R \to S$, we obtain a map on spectra $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ 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.

We observe that this is not only an order-preserving map, but also is continuous: if $U \subseteq \operatorname{Spec}(R)$ is open, we have $U = \operatorname{Spec}(R) \smallsetminus V(I)$ for some ideal I; then for a prime $\mathfrak{q}$ of S,

$$\mathfrak{q} \in (\varphi^*)^{-1}(U) \quad \Leftrightarrow \quad \mathfrak{q} \cap R \not\supseteq I \quad \Leftrightarrow \quad \mathfrak{q} \not\supseteq IS \quad \Leftrightarrow \quad \mathfrak{q} \in \operatorname{Spec}(S) \smallsetminus V(IS).$$

Lemma 4.23. *Let R be a ring, I an ideal, and W a multiplicatively closed subset. If $W \cap I = \varnothing$, then there is a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \supseteq I$ and $\mathfrak{p} \cap W = \varnothing$.*

Proof. Consider the family of ideals $\{J \mid J \supseteq I, J \cap W = \varnothing\}$. This is nonempty, since it contains I, and has some maximal element $\mathfrak{A}$ by a basic application of Zorn's Lemma. We claim $\mathfrak{A}$ is prime. Suppose $f, g \notin \mathfrak{A}$. By maximality, $\mathfrak{A} + (f)$ and $\mathfrak{A} + (g)$ both have nonempty intersection with W, so there exist $r_1 f + a_1$, $r_2 g + a_2 \in W$, with $a_1, a_2 \in \mathfrak{A}$. If $fg \in \mathfrak{A}$, then $(r_1 f + a_1)(r_2 g + a_2) = r_1 r_2 fg + r_1 f a_2 + r_2 g a_1 + a_1 a_2 \in W \cap \mathfrak{A}$, a contradiction. □

Proposition 4.24 (Spectrum analogue of strong Nullstellensatz)**.** *Let R be a ring, and I be an ideal. For $f \in R$,*

$$V(I) \subseteq V(f) \Longleftrightarrow f \in \sqrt{I}.$$

Equivalently, $\bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}$.

Lecture of February 21, 2022

Proof. First to justify the equivalence of the two statements we observe:

$$V(I) \subseteq V(f) \Leftrightarrow f \in \mathfrak{p} \text{ for all } \mathfrak{p} \in V(I) \Leftrightarrow f \in \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}.$$

We prove the latter formulation.

($\supseteq$): It suffices to show that $\mathfrak{p} \supseteq I$ implies that $\mathfrak{p} \supseteq \sqrt{I}$. But, $f^n \in \mathfrak{p}$ implies $f \in \mathfrak{p}$, so this is clear.

($\subseteq$): If $f \notin \sqrt{I}$, consider the multiplicatively closed set $W = \{1, f, f^2, f^3, \dots\}$. We have $W \cap I = \varnothing$ by hypothesis. By the previous lemma, there is a prime $\mathfrak{p}$ in $V(I)$ that does not intersect W, and hence does not contain f. □

Corollary 4.25. *For two ideals I, J, $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.*

Proof. ($\Leftarrow$): Follows from $V(I) = V(\sqrt{I})$. ($\Rightarrow$): If $V(I) = V(J)$, then $f \in \sqrt{I}$ if and only if $V(f) \supseteq V(I) = V(J)$ if and only if $f \in \sqrt{J}$. □

We also have the following:

Proposition 4.26. *$V(I)$ is irreducible if and only if $\sqrt{I}$ is prime.*

Proof. Observe first that

$$V(I + (f)) \cup V(I + (g)) = V(I^2 + (f, g)I + (fg)) = V(I^2 + (f, g)I) \cap V(fg) = V(I) \cap V(fg)$$

since $I^2 \subseteq I^2 + (f, g)I \subseteq I$ implies $\sqrt{I} = \sqrt{I^2} \subseteq \sqrt{I^2 + (f, g)I} \subseteq \sqrt{I}$ so equality holds throughout.

Now, if $\sqrt{I}$ is not prime, take $f, g \notin \sqrt{I}$ with $fg \in \sqrt{I}$. Then $V(I + (f)), V(I + (g)) \subsetneq V(I)$ and $V(I + (f)) \cup V(I + (g)) = V(I) \cap V(fg) = V(I)$ since $V(fg) \supseteq V(I)$. Thus $V(I)$ is reducible.

On the other hand, any closed proper subset of $V(I)$ is contained in a closed set of the form $V(I + (h))$ for some $h \notin \sqrt{I}$, so if $V(I)$ is reducible, then we can write $V(I) = V(I + (f)) \cup V(I + (g))$ for $f, g \notin \sqrt{I}$. By the computation above, we have $V(I) = V(I) \cap V(fg)$ so $V(fg) \supseteq V(I)$ and $fg \in \sqrt{I}$, so $\sqrt{I}$ is not prime. □

We conclude

Corollary 4.27. *Let R a ring. The map $\xrightarrow{V}$ induces order-reversing bijections*

$$\begin{array}{ccc} \underline{\text{in } R} & & \underline{\text{in } \operatorname{Spec}(R)} \\ \{\textit{radical ideals}\} & \longleftrightarrow & \{\textit{closed subsets}\} \\ \{\textit{prime ideals}\} & \longleftrightarrow & \{\textit{irred closeds}\} \\ \{\textit{maximal ideals}\} & \longleftrightarrow & \{\textit{closed points}\}. \end{array}$$

5. Support of modules and associated primes

5.1. **Localization.** Our three most important classes of examples of multiplicative sets are as follows.

Example 5.1. Let R be a ring.

(1) For any $f \in R$, the set $W = \{1, f, f^2, f^3, \dots\}$ is a multiplicative set.
(2) If $\mathfrak{p} \subseteq R$ is a prime ideal, the set $W = R \smallsetminus \mathfrak{p}$ is multiplicative: this is an immediate translation of the definition.
(3) The set of *nonzerodivisors* in R—elements that are not zerodivisors—forms a multiplicatively closed subset.

Definition 5.2 (Localization of a ring)**.** Let R be a ring, and W be a multiplicative set with $0 \notin W$. The *localization* of R at W is the ring

$$W^{-1}R := \left\{ \frac{r}{w} \;\middle|\; r \in R, w \in W \right\} / \sim$$

where $\sim$ is the equivalence relation $\dfrac{r}{w} \sim \dfrac{r'}{w'}$ if $\exists u \in W : u(rw' - r'w) = 0$. The operations are given by

$$\frac{r}{v} + \frac{s}{w} = \frac{rw + sv}{vw} \qquad \text{and} \qquad \frac{r}{v}\frac{s}{w} = \frac{rs}{vw}.$$

There is a canonical ring homomorphism $R \to W^{-1}R$ that sends $r \mapsto \frac{r}{1}$.

Note that we write elements in $W^{-1}R$ in the form r/w even though they are equivalence classes of such expressions.

Observe that if R is a domain, the equivalence relation simplifies to $rw' = r'w$, so $R \subseteq W^{-1}R \subseteq \operatorname{Frac}(R)$, and in particular $W^{-1}R$ is a domain too.

Example 5.3 (Most important localizations)**.** Let R be a ring.

(1) For $f \in R$ and $W = \{1, f, f^2, f^3, \dots\}$, we usually write R_f for $W^{-1}R$.
(2) For $\mathfrak{p} \subset R$ prime, we generally write $R_{\mathfrak{p}}$ for $(R \smallsetminus \mathfrak{p})^{-1}R$.
(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.

We state an analogous definition for modules, and for module homomorphisms.

Definition 5.4. Let R be a ring, W be a multiplicative set, and M an R-module. The *localization* of M at W is the $W^{-1}R$-module

$$W^{-1}M := \left\{ \frac{m}{w} \;\middle|\; m \in M, w \in W \right\} / \sim$$

where $\sim$ is the equivalence relation $\frac{m}{w} \sim \frac{m'}{w'}$ if $\exists u \in W : u(mw' - m'w) = 0$. The operations are given by

$$\frac{m}{v} + \frac{n}{w} = \frac{mw + nv}{vw} \qquad \text{and} \qquad \frac{r}{v}\frac{m}{w} = \frac{rm}{vw}.$$

If $M \xrightarrow{\alpha} N$ is an R-module homomorphism, then there is a $W^{-1}R$-module homomorphism $W^{-1}M \xrightarrow{W^{-1}\alpha} W^{-1}N$ given by the rule $W^{-1}\alpha(m/w) = \alpha(m)/w$.

We will use the notations M_f and $M_{\mathfrak{p}}$ analogously to R_f and $R_{\mathfrak{p}}$.

To understand localizations of rings and modules, we will want to understand better how they are built from R.

Lemma 5.5. *Let M be an R-module, and W a multiplicative set. The class*

$$\frac{m}{w} \in W^{-1}M \text{ is zero} \iff \exists v \in W \ : \ vm = 0 \iff \operatorname{ann}_R(m) \cap W \neq \varnothing.$$

Note in particular this holds for $w = 1$.

Proof. For the first equivalence, we compute: $\frac{m}{w} = \frac{0}{1}$ in $W^{-1}M$ if and only if $\exists v \in W$ such that $0 = v(1m - 0w) = vm$. The second equivalence just comes from the definition of the annihilator. □

Remark 5.6. It follows from this lemma that if $\alpha : N \to M$ is injective, then $W^{-1}\alpha : W^{-1}N \to W^{-1}M$ is as well. Indeed, if α is injective, then

$$0 = W^{-1}\alpha(n/w) = \alpha(n)/w \ \Rightarrow \ \exists u \in W : 0 = u\alpha(n) = \alpha(un) \Rightarrow \ un = 0 \Rightarrow n/w = 0.$$

We want to collect one more lemma for later.

Lemma 5.7. *Let M be a module, and $N_1, \dots, N_t$ be a finite collection of submodules. Let W be a multiplicative set. Then,*

$$W^{-1}(N_1 \cap \cdots \cap N_t) = W^{-1}N_1 \cap \cdots \cap W^{-1}N_t \subseteq W^{-1}M.$$

Proof. The containment "$\subseteq$" is clear. An element of the RHS is of the form $\frac{n_1}{w_1} = \cdots = \frac{n_t}{w_t}$; we can find a common denominator to realize this in the LHS. □

Last semester in the homework we showed the following.

Theorem 5.8 (Flatness of localization)**.** *Let R be a ring, and W a multiplicative system. Then*

1. *$W^{-1}R \otimes_R M \cong W^{-1}M$ as $W^{-1}R$-modules, and $W^{-1}R \otimes \alpha$ corresponds to $W^{-1}\alpha$ under these isomorphisms.*
2. *$W^{-1}R$ is flat over R.*
3. *$W^{-1}(-)$ is an exact functor; i.e., it sends exact sequences to exact sequences.*

Proposition 5.9. *Let W be multiplicatively closed in R.*

0. *$W^{-1}I = I(W^{-1}R)$.*
1. *If I is an ideal, then $W^{-1}I \cap R = \{r \in R \mid \exists w \in W : wr \in I\}$.*
2. *If $\mathfrak{p}$ is prime and $W \cap \mathfrak{p} = \varnothing$, then $W^{-1}\mathfrak{p} = \mathfrak{p}(W^{-1}R)$ is prime.*
3. *The map $\operatorname{Spec}(W^{-1}R) \to \operatorname{Spec}(R)$ is injective, with image $\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}$.*

Proof. (1) Since $W^{-1}(R/I) \cong W^{-1}R/W^{-1}I$, we have $\ker(R \to W^{-1}(R/I)) = R \cap W^{-1}I$. The equality is then clear.

(2) First, since $W \cap \mathfrak{p} = \varnothing$, and $\mathfrak{p}$ is prime, we know that no element of W kills $\bar{1} = 1 + \mathfrak{p}$ in $R/\mathfrak{p}$, so $\bar{1}/1$ is nonzero in $W^{-1}(R/\mathfrak{p})$. Thus, $W^{-1}R/W^{-1}\mathfrak{p} \cong W^{-1}(R/\mathfrak{p})$ nonzero, and a localization of a domain, hence is a domain. Thus, $W^{-1}\mathfrak{p}$ is prime.

Lecture of February 23, 2022

(3) First, by part (2), the map $\mathfrak{p} \mapsto W^{-1}\mathfrak{p}$, for $S = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}$ sends primes to primes. We claim that

$$\operatorname{Spec}(W^{-1}R) \longleftrightarrow S$$

$$\mathfrak{q} \longmapsto \mathfrak{q} \cap R$$

$$W^{-1}\mathfrak{p} = \mathfrak{p}(W^{-1}R) \longmapsfrom \mathfrak{p}$$

is a pair of mutually inverse maps.

To see this, first note that if J is an ideal of $W^{-1}R$, then $J = (J \cap R)W^{-1}R$. Indeed, if $J = (a_1/w_1, \ldots, a_t/w_t)$, then $J = (a_1/1, \ldots, a_t/1)$, since each generator was replaced by a unit multiple. Second, if $W \cap \mathfrak{p} = \varnothing$, then using part (1) and the definition of prime, we have that $\mathfrak{p} = W^{-1}\mathfrak{p} \cap R$. □

Corollary 5.10. *Let R be a ring and $\mathfrak{p}$ be a prime ideal. The map $R \to R_{\mathfrak{p}}$ induces a map on spectra that is injective with image*

$$\{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\}.$$

Proposition 5.11 (Hom and flat base change)**.** *Let S be a flat R algebra, and M, N be two R-modules. Suppose that M is finitely presented. Then*

$$S \otimes_R \operatorname{Hom}_R(M, N) \xrightarrow{\cong} \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

$$s \otimes \varphi \longmapsto s(S \otimes \varphi)$$

is an isomorphism.

Proof. When M is R or a finitely generated free module $R^{\oplus a}$, this is clear: both sides are isomorphic to $(S \otimes_R N)^{\oplus a}$, and it is easy to see that the map above realizes this.

Now, take a presentation

$$R^{\oplus b} \to R^{\oplus a} \to M \to 0.$$

If we apply $S \otimes_R -$, we obtain another right exact sequence; if we then apply $\operatorname{Hom}_S(-, S \otimes_R N)$ to this presentation, we obtain a left-exact sequence

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^{\oplus a}, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^{\oplus b}, S \otimes_R N).$$

Likewise, if we apply $\operatorname{Hom}_R(-, N)$, we obtain a left exact sequence; if we then apply $S \otimes_R -$, we obtain by flatness another left exact sequence

$$0 \to S \otimes_R \operatorname{Hom}_R(M, N) \to S \otimes_R \operatorname{Hom}_R(R^{\oplus a}, N) \to \operatorname{Hom}_R(R^{\oplus b}, N).$$

We then have a diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N) & \longrightarrow & \mathrm{Hom}_S(S\otimes_R R^{\oplus a}, S\otimes_R N) & \longrightarrow & \mathrm{Hom}_S(S\otimes_R R^{\oplus b}, S\otimes_R N) \\
 & & \uparrow & & \cong\uparrow & & \cong\uparrow \\
0 & \longrightarrow & S\otimes_R \mathrm{Hom}_R(M,N) & \longrightarrow & S\otimes_R \mathrm{Hom}_R(R^{\oplus a},N) & \longrightarrow & S\otimes_R \mathrm{Hom}_R(R^{\oplus b},N),
\end{array}$$

where the vertical maps are given by the formula of the statement. We claim that the squares commute. Indeed, given $X \xrightarrow{\alpha} Y$,

$$\begin{array}{ccc}
\mathrm{Hom}_S(S\otimes_R Y, S\otimes_R N) & \xrightarrow{\mathrm{Hom}(S\otimes\alpha, S\otimes N)} & \mathrm{Hom}_S(S\otimes_R X, S\otimes_R N)\ , \\
\uparrow & & \uparrow \\
S\otimes_R \mathrm{Hom}_R(Y,N) & \xrightarrow{S\otimes\mathrm{Hom}(\alpha,N)} & S\otimes_R \mathrm{Hom}_R(X,N)
\end{array}$$

an element $s\otimes\varphi$ in the bottom left goes $\uparrow$ to $s\cdot(S\otimes\varphi)$ and then $\rightarrow$ to $s\cdot(S\otimes(\varphi\circ\alpha))$, whereas $s\otimes\varphi$ goes $\rightarrow$ to $s\otimes(\varphi\circ\alpha)$ and then $\uparrow$ to $s\cdot(S\otimes(\varphi\circ\alpha))$. It then follows that there is an isomorphism in the first vertical map in the previous diagram. □

Corollary 5.12 (Hom and localization)**.** *Let R be a Noetherian ring, W be a multiplicative set, M be a finitely generated R-module, and N an arbitrary R-module. Then,*

$$\mathrm{Hom}_{W^{-1}R}(W^{-1}M, W^{-1}N) \cong W^{-1}\mathrm{Hom}_R(M,N).$$

In particular, if $\mathfrak{p}$ is prime,

$$\mathrm{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \cong \mathrm{Hom}_R(M,N)_\mathfrak{p}.$$

5.2. **Minimal primes and support.**

Definition 5.13. The primes that contain I and are minimal with the property of containing I are called the *minimal primes* of I. That is, the minimal primes of I are the minimal elements of $V(I)$. We write $\mathrm{Min}(I)$ for this set.

Remark 5.14. If $\mathfrak{p}$ is prime, then $\mathrm{Min}(\mathfrak{p}) = \{\mathfrak{p}\}$. Also, since $V(I) = V(\sqrt{I})$, we have $\mathrm{Min}(I) = \mathrm{Min}(\sqrt{I})$.

Remark 5.15. As a consequence of the order-reversing correspondence between irreducible closed subsets and prime ideals, for an ideal I and a prime ideal $\mathfrak{p}$, we have that $\mathfrak{p} \in \mathrm{Min}(I)$ if and only if $V(\mathfrak{p})$ is an irreducible component of $V(I)$.

Theorem 5.16. *Let R be a ring and I be an ideal.*

(1) *Every prime containing I contains a minimal prime of I. Consequently,*

$$\sqrt{I} = \bigcap_{\mathfrak{p}\in\mathrm{Min}(I)} \mathfrak{p}.$$

(2) *If $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ with each $\mathfrak{p}_i$ prime, and $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $i \neq j$, then $\mathrm{Min}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

(3) *If R is Noetherian, then $\mathrm{Min}(I)$ is finite. Hence, if R is Noetherian, $\sqrt{I}$ can be written as a finite irredundant intersection of primes in a unique way.*

Proof. We can prove these directly, but we can instead deduce them for our general proposition on irreducible components of topological spaces and the remarks above.

For (1), we recall that a topological space is the union of its irreducible components, so in particular, each point $\mathfrak{q} \in V(I)$ is contained in a set of the form $V(\mathfrak{p})$ for some minimal prime $\mathfrak{p} \in \operatorname{Min}(I)$, which means $\mathfrak{q}$ contains a minimal prime.

For (2), we have $V(I) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_n)$; if $V(\mathfrak{p}_i) \subseteq \bigcup_{j \neq i} V(\mathfrak{p}_j)$, then $\mathfrak{p}_i \in V(\mathfrak{p}_j)$ for some j, so $\mathfrak{p}_i \supseteq \mathfrak{p}_j$. Thus, our union of closed subsets is irredundant, so $\{V(\mathfrak{p}_1), \ldots, V(\mathfrak{p}_n)\}$ must be the set of irreducible components, and the statement follows.

For (3), since $\operatorname{Spec}(R)$ is Noetherian, any closed set $V(I)$ has finitely many irreducible components, and the statement follows. □

Lecture of February 25, 2022

As a special case of part (1), the nilpotent elements of a ring R are exactly the elements in every minimal prime of R, or equivalently, in every minimal prime of the ideal (0). The ideal $\sqrt{(0)}$ is called the *nilradical* of R. That is,

Remark 5.17. If R is Noetherian, then any closed set $V(I)$ is the union of finitely many sets of the form $V(\mathfrak{p})$ for primes $\mathfrak{p}$.

We now wish to understand modules in a similar way.

Definition 5.18. If M is an R-module, the *support* of M is

$$\operatorname{Supp}(M) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}.$$

Proposition 5.19. *Given M a finitely generated R-module over a ring R,*

$$\operatorname{Supp}(M) = V(\operatorname{ann}_R(M)).$$

In particular, $\operatorname{Supp}(R/I) = V(I)$.

Proof. Let $M = Rm_i + \cdots + Rm_n$. We have

$$\operatorname{ann}_R(M) = \bigcap_{i=1}^{n} \operatorname{ann}_R(m_i),$$

so

$$V(\operatorname{ann}_R(M)) = \bigcup_{i=1}^{n} V(\operatorname{ann}_R(m_i)).$$

Notice that we need finiteness here. Also, we claim that

$$\operatorname{Supp}(M) = \bigcup_{i=1}^{n} \operatorname{Supp}(Rm_i).$$

To show ($\supseteq$), notice that $(Rm_i)_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$, so

$$\mathfrak{p} \in \operatorname{Supp}(Rm_i) \implies 0 \neq (Rm_i)_{\mathfrak{p}} \subseteq M_{\mathfrak{p}} \implies \mathfrak{p} \in \operatorname{Supp}(M).$$

On the other hand, the images of $m_1, \ldots, m_n$ in $M_{\mathfrak{p}}$ generate $M_{\mathfrak{p}}$ for each $\mathfrak{p}$, so $\mathfrak{p} \in \operatorname{Supp}(M)$ if and only if $\mathfrak{p} \in \operatorname{Supp}(Rm_i)$ for some m_i. Thus, we can reduce to the case of a cyclic module Rm. Now $\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ if and only if $(R \smallsetminus \mathfrak{p}) \cap \operatorname{ann}_R(m) \neq \varnothing$, which happens if and only if $\operatorname{ann}_R(m) \nsubseteq \mathfrak{p}$. □

The finite generating hypothesis is necessary!

Example 5.20. Let K be a field, and $R = K[x]$. Take

$$M = R_x/R = \bigoplus_{i>0} K \cdot x^{-i}.$$

With this K-vector space structure, the action is given by multiplication in the obvious way, then killing any nonnegative degree terms.

On one hand, we claim that $\mathrm{Supp}(M) = \{(x)\}$. Indeed, any element of M is killed by a large power of x, so $W^{-1}M = 0$ whenever $x \in W$, so $\mathrm{Supp}(M) \subseteq \{(x)\}$. Since $\mathrm{ann}_R(x^{-1}) = (x)$, the image of x^{-1} is nonzero in $M_{(x)}$, so $\mathrm{Supp}(M) = \{(x)\}$.

On the other hand, the annihilator of the class of x^{-n} is x^n, so

$$\mathrm{ann}_R(M) \subseteq \bigcap_{n \geqslant 1} (x^n) = 0.$$

In particular, $V(\mathrm{ann}_R(M)) = \mathrm{Spec}(R)$.

Example 5.21. Let $R = \mathbb{C}[x]$, and $M = \bigoplus_{n \in \mathbb{Z}} R/(x-n)$.

First, note that $M_{\mathfrak{p}} = \bigoplus_{n \in \mathbb{Z}} (R/(x-n))_{\mathfrak{p}}$, so

$$\mathrm{Supp}(M) = \bigcup_{n \in \mathbb{Z}} \mathrm{Supp}(R/(x-n)) = \bigcup_{n \in \mathbb{Z}} V((x-n)) = \{(x-n) \mid n \in \mathbb{Z}\}.$$

On the other hand,

$$\mathrm{ann}_R(M) = \bigcap_{n \in \mathbb{Z}} \mathrm{ann}_R(R/(x-n)) = \bigcap_{n \in \mathbb{Z}} (x-n) = 0.$$

Note that in this example the support is not even closed.

Lemma 5.22. *Let R be a ring, M an R-module, and $m \in M$. The following are equivalent:*

1. *$m = 0$ in M.*
2. *$\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$.*
3. *$\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Max}(R)$.*

Proof. The implications 1) $\implies$ 2) $\implies$ 3) are clear. If $m \neq 0$, its annihilator is a proper ideal, which is contained in a maximal ideal, so $V(\mathrm{ann}_R\, m) = \mathrm{Supp}(Rm)$ contains a maximal ideal, so $\frac{m}{1} \neq 0$ in $M_{\mathfrak{p}}$ for some maximal ideal $\mathfrak{p}$. □

Optional Exercise 5.23. If

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

is exact, then $\mathrm{Supp}(L) \cup \mathrm{Supp}(N) = \mathrm{Supp}(M)$.

Optional Exercise 5.24. If M is a finitely generated R-module,

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$.
3. $M_{\mathfrak{p}} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Max}(R)$.

5.3. **Associated primes.**

Definition 5.25. Let R be a ring, and M a module. We say that $\mathfrak{p} \in \mathrm{Spec}(R)$ is an *associated prime* of M if $\mathfrak{p} = \mathrm{ann}_R(m)$ for some $m \in M$. Equivalently, $\mathfrak{p}$ is associated to M if there is an injective homomorphism $R/\mathfrak{p} \longrightarrow M$. We write $\mathrm{Ass}_R(M)$ for the set of associated primes of M.

If I is an ideal, by the *associated primes* of I we (almost always) mean the associated primes of R/I. To avoid confusion, we will try to write $\mathrm{Ass}_R(R/I)$.

Lemma 5.26. *If $\mathfrak{p}$ is prime, $\mathrm{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.*

Proof. For any nonzero $\bar{r} \in R/\mathfrak{p}$, we have $\operatorname{ann}_R(\bar{r}) = \{s \in R \mid rs \in \mathfrak{p}\} = \mathfrak{p}$ by definition of prime ideal. □

Let's recall the definition of zerodivisors on M.

Definition 5.27. Let M be an R-module. An element $r \in R$ is a **zerodivisor** on M if $rm = 0$ for some $m \in M$.

Lemma 5.28. *If R is Noetherian, and M is an arbitrary R-module, then*

(1) *For any nonzero $m \in M$, $\operatorname{ann}_R(m)$ is contained in an associated prime of M.*
(2) $\operatorname{Ass}(M) = \varnothing \iff M = 0$, *and*
(3) $\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p}$ *is the set of zerodivisors on M.*

Proof. (1) The set of ideals $S := \{\operatorname{ann}_R(m) \mid m \in M, m \neq 0\}$ is nonempty, and any element in S is contained in a maximal element of S, by Noetherianity. Let $I = \operatorname{ann}(m)$ be any maximal element, and let $rs \in I$, $s \notin I$. We always have $\operatorname{ann}(sm) \supseteq \operatorname{ann}(m)$, and equality holds by the maximality of $\operatorname{ann}(m)$ in S. Then $r(sm) = (rs)m = 0$, so $r \in \operatorname{ann}(sm) = \operatorname{ann}(m) = I$. We conclude that I is prime, and therefore it is an associated prime of M.

(2) Even if R is not Noetherian, $M = 0$ implies $\operatorname{Ass}(M) = \varnothing$ by definition. So we focus on the case when $M \neq 0$. If $M \neq 0$, then M contains a nonzero element m, and $\operatorname{ann}(m)$ is contained in an associated prime of M. In particular, $\operatorname{Ass}(M) \neq 0$, and holds.

(3) Now if $r \in \mathcal{Z}(M)$, then by definition we have $r \in \operatorname{ann}(m)$ for some nonzero $m \in M$. Since $\operatorname{ann}(m)$ is contained in some associated prime of M, so is r. On the other hand, if $\mathfrak{p}$ is an associated prime of M, then by definition all elements in $\mathfrak{p}$ are zerodivisors on M. □

Lecture of February 28, 2022

Example 5.29. If R is not Noetherian, then there may be modules (or ideals even) with no associated primes. Let $R = \bigcup_{n \in \mathbb{N}} \mathbb{C}[\![x^{1/n}]\!]$ be the ring of nonnegatively-valued Puiseux series. We claim that $R/(x)$ is a cyclic module with no associated primes (i.e., the ideal (x) has no associated primes). First, observe that any element of R can be written as a unit times $x^{m/n}$ for some m, n, so any associated prime must be an annihilator of $x^{m/n} + (x)$ for some $m \leqslant n$. We have $\operatorname{ann}(x^{m/n} + (x)) = (x^{1-m/n})$, which is not prime, since $(x^{1/2-m/2n})^2 \in (x^{1-m/n})$, but $x^{1/2-m/2n}$.

For Noetherian rings, associated primes also localize.

Theorem 5.30 (Associated primes localize in Noetherian rings)**.** *Let R be a Noetherian ring, W a multiplicative set, and M a module. Then* $\operatorname{Ass}_{W^{-1}R}(W^{-1}M) = \{W^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M), \mathfrak{p} \cap W = \varnothing\}$.

Proof. ($\supseteq$): Given $\mathfrak{p} \in \operatorname{Ass}_R(M), \mathfrak{p} \cap W = \varnothing$, we have that $W^{-1}\mathfrak{p}$ is a prime (proper ideal) in $W^{-1}R$. Then $W^{-1}R/W^{-1}\mathfrak{p} \cong W^{-1}(R/\mathfrak{p}) \hookrightarrow W^{-1}M$ by exactness, so it is associated.

($\subseteq$): If $W^{-1}\mathfrak{p}$ is associated to $W^{-1}M$, there is an embedding

$$W^{-1}(R/\mathfrak{p}) (\cong W^{-1}R/W^{-1}\mathfrak{p}) \xrightarrow{i} W^{-1}M.$$

By the Noetherian hypothesis, since $R/\mathfrak{p}$ is finitely generated, Hom localizes: $W^{-1}\operatorname{Hom}_R(R/\mathfrak{p}, M) \cong \operatorname{Hom}_{W^{-1}R}(W^{-1}R/W^{-1}\mathfrak{p}, W^{-1}M)$, so there is some $R/\mathfrak{p} \xrightarrow{i'} M$ and $w \in W$ such that $i = w^{-1} \cdot W^{-1}i'$. Let $K = \ker(i')$. Since $W^{-1}K = \ker(W^{-1}i) = 0$ by exactness, every element of K is killed by something in W. But, $K \subseteq R/\mathfrak{p}$, so elements of W act as nonzerodivisors on K. Hence, $K = 0$. Thus, $R/\mathfrak{p}$ injects into M, so $\mathfrak{p} \in \operatorname{Ass}_R(M)$. □

Proposition 5.31. *Let R be a Noetherian ring and M be an R-module.*

(1) $\operatorname{Supp}_R(M) = \bigcup_{\mathfrak{p}\in \operatorname{Ass}_R(M)} V(\mathfrak{p})$
(2) $\min(\operatorname{Supp}_R(M)) = \min(\operatorname{Ass}_R(M))$

In particular, $\operatorname{Min}(I) = \min(\operatorname{Ass}_R(R/I))$.

Proof. (1) We have $\mathfrak{p} \in \operatorname{Supp}_R(M)$ iff $M_\mathfrak{p} \neq 0$ iff $\operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq \varnothing$ iff $\operatorname{Ass}_R(M) \cap \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} = \varnothing$ iff M contains an associated prime of M.

(2) Let $\mathfrak{p} \in \min(\operatorname{Supp}_R(M))$. Then there is some $\mathfrak{q} \in \operatorname{Ass}_R(M)$ with $\mathfrak{q} \subseteq \mathfrak{p}$. If $\mathfrak{q} \subsetneqq \mathfrak{p}$, then $\mathfrak{q} \in \operatorname{Supp}_R(M)$ contradicts minimality of $\mathfrak{p}$, so $\mathfrak{p} = \mathfrak{q} \in \operatorname{Ass}_R(M)$. If $\mathfrak{p}$ is not minimal in $\operatorname{Ass}_R(M)$, it is not minimal in the support, so we must have $\mathfrak{p} \in \min(\operatorname{Ass}_R(M))$. On the other hand, for $\mathfrak{p} \in \min(\operatorname{Ass}_R(M))$, $\mathfrak{p}$ is in the support of M. If there is some $\mathfrak{q} \in \operatorname{Supp}_R(M)$ with $\mathfrak{q} \subsetneqq \mathfrak{p}$, then there is some $\mathfrak{r} \in \operatorname{Ass}_R(M)$ with $\mathfrak{r} \subseteq \mathfrak{q}$, contradicting minimality of $\mathfrak{p}$. Thus, $\mathfrak{p} \in \min(\operatorname{Supp}_R(M))$. □

Definition 5.32. For an ideal I, we say a prime $\mathfrak{p}$ is an *embedded prime* of I if $\mathfrak{p} \in \operatorname{Ass}_R(R/I) \smallsetminus \operatorname{Min}(I)$.

Lemma 5.33. *If $0 \to L \to M \to N \to 0$ is exact, then* $\operatorname{Ass}(L) \subseteq \operatorname{Ass}(M) \subseteq \operatorname{Ass}(L) \cup \operatorname{Ass}(N)$.

Proof. If $R/\mathfrak{p} \hookrightarrow L$, then composition with the inclusion $L \hookrightarrow M$ gives $R/\mathfrak{p} \hookrightarrow M$. Let $\mathfrak{p} \in \operatorname{Ass}(M) \smallsetminus \operatorname{Ass}(L)$, and let $\mathfrak{p} = \operatorname{ann}(m)$. Now, every submodule of Rm consists of 0 and elements with annihilator $\mathfrak{p}$, so $Rm \cap L = 0$. Thus, $Rm \subseteq M$ bijects onto its image in N in the map $M \to N$, so $R/\mathfrak{p} \hookrightarrow N$. □

Lecture of March 2, 2022

Theorem 5.34. *If R is a Noetherian ring, and M is a finitely generated module, then there exists a* filtration *of M*

$$M = M_t \supsetneqq M_{t-1} \supsetneqq M_{t-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$. Such a filtration is called a prime filtration *of M.*

Proof. If $M \neq 0$, then M has an associated prime, so there is an injection $M_1 \cong R/\mathfrak{p}_1 \hookrightarrow M$. If $M/M_1 \neq 0$, it has an associated prime, so there is an $M_2 \subseteq M$ such that $M_2/M_1 \cong R/\mathfrak{p}_2 \hookrightarrow R/M_1$. Continuing this process, we get a strictly ascending chain of submodules of M where the successive quotients are of the form $R/\mathfrak{p}_i$. If we do not have $M_t = M$ for some t, then we get an infinite strictly ascending chain of submodules of M, which contradicts that M is a Noetherian module. □

Corollary 5.35. *If R is a Noetherian ring, and M is a finitely generated module, and*

$$M = M_t \supsetneqq M_{t-1} \supsetneqq M_{t-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

is a prime filtration of M with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ then

$$\operatorname{Ass}_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}.$$

Consequently, $\operatorname{Ass}_R(M)$ *is finite.*

Proof. For each i, we have $\operatorname{Ass}(M_i) \subseteq \operatorname{Ass}(M_{i-1}) \cup \operatorname{Ass}(M_i/M_{i-1}) = \operatorname{Ass}(M_{i-1}) \cup \{\mathfrak{p}_i\}$ so that, inductively, $\operatorname{Ass}(M_i) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_i\}$. The consequencenfollows from the previous theorem. □

Lemma 5.36 (Prime avoidance)**.** *Let R be a ring, $I_1, \ldots, I_n, J$ be ideals, and suppose that I_i is prime for $i > 2$ (at most two are not prime).*

If $J \nsubseteq I_i$ for all i, then $J \nsubseteq \bigcup_i I_i$; equivalently, if $J \subseteq \bigcup_i I_i$, then $J \subseteq I_i$ for some i.

Moreover, if R is $\mathbb{N}$-graded, and all of the ideals are homogeneous, all I_i are prime, and $J \nsubseteq I_i$ for all i, then there is a homogeneous element in $J \smallsetminus \bigcup_i I_i$.

Proof. We proceed by induction on n. If $n = 1$, there is nothing to show.

By induction hypothesis, we can find elements $a_i \in J \smallsetminus \bigcup_{j\neq i} I_j$ for each i. If some $a_i \notin I_i$, we are done, so suppose that $a_i \in I_i$ for each i. Consider $a = a_n + a_1 \cdots a_{n-1}$. This belongs to J. If $a \in I_i$ for $i < n$, then, since $a_1 \cdots a_{n-1} = a_i(a_1 \cdots \widehat{a_i} \cdots a_{n-1}) \in I_i$, we also have $a_n \in I_i$, a contradiction. If $a \in I_n$, then, since $a_n \in I_n$, we also have $a_1 \cdots a_{n-1} \in I_n$. If $n = 2$, this says $a_1 \in I_2$, a contradiction. If $n > 2$, then I_n is prime, so one of $a_1, \ldots, a_{n-1} \in I_n$, a contradiction.

If all I_i are homogeneous and prime, we proceed as above, replacing a_n and $a_1, \ldots, a_{n-1}$ with suitable powers (e.g., $|a_1| + \cdots + |a_{n-1}|$ and $|a_n|$ each, respectively) so that $a_n + a_1 \cdots a_{n-1}$ is homogeneous. The primeness assumption guarantees that noncontainments in ideals is preserved. □

Corollary 5.37. *Let I be an ideal and M a finitely generated module over a Noetherian ring R. If I consists of zerodivisors on M, then $Im = 0$ for some $m \in M$.*

Proof. We have that $I \subseteq \bigcup_{\mathfrak{p}\in \mathrm{Ass}(M)}(\mathfrak{p})$. By the assumptions, this is a finite set of primes. By prime avoidance, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M)$. That is $I \subseteq \mathrm{ann}_R(m)$ for some $m \in M$. □

Lecture of March 4, 2022

5.4. **Primary decomposition.** We refine our decomposition theory once again, and introduce primary decompositions of ideals.

Definition 5.38. We say that an ideal is *primary* if

$$xy \in I \implies x \in I \text{ or } y \in \sqrt{I}.$$

We say that an ideal is $\mathfrak{p}$-*primary*, where $\mathfrak{p}$ is prime, if I is primary and $\sqrt{I} = \mathfrak{p}$.

Remark 5.39. Note that a primary ideal has indeed a prime radical: if Q is primary, and $xy \in \sqrt{Q}$, then $x^n y^n \in Q$ for some n. If $y \notin \sqrt{Q}$, then we must have $x^n \in Q$, so $x \in \sqrt{Q}$. Thus, every primary ideal Q is $\sqrt{Q}$-primary.

Example 5.40.

(1) Any prime ideal is also primary.

(2) If R is a UFD, we claim that a principal ideal is primary if and only if it is generated by a power of a prime element. Indeed, if $a = f^n$, with f irreducible, then

$$xy \in (f^n) \iff f^n | xy \iff f^n | x \text{ or } f | y \iff x \in (f^n) \text{ or } y \in \sqrt{(f^n)} = (f).$$

Conversely, if a is not a prime power, then $a = gh$, for some g, h nonunits with no common factor, then take $gh \in (a)$ but $g \notin a$ and $h \notin \sqrt{(a)}$.

(3) As a particular case of the previous example, the nonzero primary ideals in $\mathbb{Z}$ are of the form (p^n) for some prime p and some $n \geqslant 1$. This example is a bit misleading, as it suggests that primary ideals are the same as powers of primes. We will soon see that it not the case.

(4) In $R = k[x, y, z]$, the ideal $I = (y^2, yz, z^2)$ is primary. Give R the grading with weights $|y| = |z| = 1$, and $|x| = 0$. If $g \notin \sqrt{I} = (y, z)$, then g has a degree zero term. If $f \notin I$, then f has a term of degree zero or one. The product fg has a term of degree zero or one, so is not in I.

If the radical of an ideal is prime, that does not imply that ideal is primary.

Example 5.41. In $R = k[x, y, z]$, the ideal $\mathfrak{q} = (x^2, xy)$ is not primary, even though $\sqrt{\mathfrak{q}} = (x)$ is prime. The offending product is xy.

The definition of primary can be reinterpreted in many forms.

Proposition 5.42. *The following are equivalent:*

(1) $\mathfrak{q}$ *is primary.*
(2) *Every zerodivisor in* $R/\mathfrak{q}$ *is nilpotent on* $R/\mathfrak{q}$.
(3) $\sqrt{\mathfrak{q}} = \mathfrak{p}$ *is prime and for all* $r, w \in R$ *with* $w \notin \mathfrak{p}$, $rw \in \mathfrak{q}$ *implies* $r \in \mathfrak{q}$.
(4) $\sqrt{\mathfrak{q}} = \mathfrak{p}$ *is prime, and* $\mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$.

If R *is Noetherian, then these are also equivalent to:*

(5) $\operatorname{Ass}(R/\mathfrak{q})$ *is a singleton.*
(6) $\mathfrak{q}$ *has exactly one minimal prime, and no embedded primes.*

Proof. (1) $\iff$ (2): y is a zerodivisor mod $\mathfrak{q}$ if there is some $x \notin \mathfrak{q}$ with $xy \in \mathfrak{q}$; the primary assumption translates to a power of y is in $\mathfrak{q}$.

(1) $\iff$ (3): Given the observation that the radical of a primary ideal is prime, this is just a rewording of the definition.

(3) $\iff$ (4): We already know this from the discussion on behavior of ideals in localizations, which says that

$$\mathfrak{q}R_{\mathfrak{p}} \cap R = \{r \in R \mid rs \in \mathfrak{q} \text{ for some } s \notin \mathfrak{p}\}.$$

(2) $\iff$ (5): On the one hand, (2) says that the set of zerodivisors on $R/\mathfrak{q}$ and coincide with the elements in the nilradical of $R/\mathfrak{q}$. These agree with the union of all the associated primes and the intersection of all the minimal primes respectively.

$$\bigcup_{\mathfrak{p}\in\operatorname{Ass}(R/\mathfrak{q})} \mathfrak{p} = \{\text{zerodivisors on } (R/\mathfrak{q})\} = \{r \in R \mid r + \mathfrak{q} \in \text{nilradical of } (R/\mathfrak{q})\} = \bigcap_{\mathfrak{p}\in\operatorname{Min}(\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(R/\mathfrak{q})} \mathfrak{p}.$$

This holds if and only if there is only one associated prime.

(5) $\iff$ (6) follows from the definitions. □

If the radical of an ideal is maximal, that *does* imply the ideal is primary.

Remark 5.43. Let I be an ideal with $\sqrt{I} = \mathfrak{m}$ a maximal ideal. If R is Noetherian, then $\operatorname{Ass}_R(R/I)$ is nonempty and contained in $\operatorname{Supp}(R/I) = V(I) = \{\mathfrak{m}\}$, so $\operatorname{Ass}_R(R/I) = \mathfrak{m}$, and hence I is primary.

Note that the assumption that $\mathfrak{m}$ is maximal was necessary here. Indeed, having a prime radical does not guarantee an ideal is primary, as we saw above Moreover, even the powers of a prime ideal may fail to be primary.

Example 5.44. Let $R = k[x, y, z]/(xy - z^n)$, where k is a field and $n \geqslant 2$ is an integer. Consider the prime ideal $P = (x, z)$ in R, and note that $y \notin P$. On the one hand, $xy = z^n \in P^n$, while $x \notin P^n$ and $y \notin \sqrt{P^n} = P$. Therefore, P^n is not a primary ideal, even though its radical is the prime P.

The contraction of primary ideals is always primary.

Remark 5.45. Given any ring map $R \xrightarrow{\phi} S$, and a primary ideal Q in S, then the contraction of Q in R (via f) $Q \cap R$ is always primary. Indeed, if $xy \in Q \cap R$, and $x \notin Q \cap R$, then $\phi(x) \notin Q$, so $\phi(y^n) = \phi(y)^n \in Q$ for some n. Therefore, $y^n \in Q \cap R$, and $Q \cap R$ is indeed primary.

Lemma 5.46. *If $I_1, \dots, I_t$ are ideals, then*

$$\operatorname{Ass}\left(R/\bigcap_{j=1}^{t} I_j\right) \subseteq \bigcup_{j=i}^{t} \operatorname{Ass}(R/I_j).$$

In particular, a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

Proof. There is an inclusion $R/(I_1 \cap I_2) \subseteq R/I_1 \oplus R/I_2$. Hence, $\operatorname{Ass}(R/(I_1 \cap I_2)) \subseteq \operatorname{Ass}(R/I_1) \cup \operatorname{Ass}(R/I_2)$; the statement for larger t is an easy induction.

If the I_j are all $\mathfrak{p}$-primary, then

$$\operatorname{Ass}(R/(\bigcap_{j=1}^{t} I_j)) \subseteq \bigcup_{j=i}^{t} \operatorname{Ass}(R/I_j) = \{\mathfrak{p}\}.$$

On the other hand, $\bigcap_{j=1}^{t} I_j \subseteq I_1 \neq R$, so $R/(\bigcap_{j=1}^{t} I_j) \neq 0$. Thus $\operatorname{Ass}(R/(\bigcap_{j=1}^{t} I_j))$ is nonempty, and therefore the singleton $\{\mathfrak{p}\}$. Then $\bigcap_{j=1}^{t} I_j$ is $\mathfrak{p}$-primary by the characterization of primary in 5.42 (3) above. □

Definition 5.47 (Primary decomposition)**.** A *primary decomposition* of an ideal I is an expression of the form

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t,$$

with each $\mathfrak{q}_i$ primary. A *minimal primary decomposition* of an ideal I is a primary decomposition as above in which $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ for $i \neq j$, and $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for all i.

Remark 5.48. By the previous lemma, we can turn any primary decomposition into a minimal one by combining the terms with the same radical, then removing redundant terms.

Lecture of March 7, 2022

Example 5.49 (Primary decomposition in $\mathbb{Z}$)**.** Given a decomposition of $n \in \mathbb{Z}$ as a product of distinct primes, say $n = p_1^{a_1} \cdots p_k^{a_k}$, then the primary decomposition of the ideal (n) is $(n) = (p_1^{a_1}) \cap \cdots \cap (p_k^{a_k})$. Note that primary is not the same is prime power in general.

Example 5.50. If R is Noetherian and I is a radical ideal, then $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ for the minimal primes $\mathfrak{p}_i$ of I. This is a minimal primary decomposition of I.

The existence of primary decompositions was first shown by Emanuel Lasker for polynomial rings and power series rings in 1905, and then extended to what we now call Noetherian rings by Emmy Noether in 1921. It will be useful to consider the following notion in the proof.

Definition 5.51. An ideal I is *irreducible* if there do not exist ideals $J_1, J_2 \supsetneq I$ such that $J_1 \cap J_2 = I$.

Theorem 5.52 (Existence of primary decompositions)**.** *Let R be a Noetherian ring.*

(1) *Every irreducible ideal is primary.*
(2) *Every ideal can be written as a finite intersection of irreducible ideals.*

Thus, every ideal of R admits a primary decomposition.

Proof. (1) To prove the contrapositive, suppose that $\mathfrak{q}$ is not primary, and take $xy \in \mathfrak{q}$ with $x \notin \mathfrak{q}$, $y \notin \sqrt{\mathfrak{q}}$. The ascending chain of ideals

$$(\mathfrak{q} : y) \subseteq (\mathfrak{q} : y^2) \subseteq (\mathfrak{q} : y^3) \subseteq \cdots$$

stabilizes for some n, since R is Noetherian. This means that $y^{n+1}f \in \mathfrak{q} \implies y^n f \in \mathfrak{q}$. We will show that

$$(\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)) = \mathfrak{q},$$

proving that $\mathfrak{q}$ is not irreducible.

The containment $\mathfrak{q} \subseteq (\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x))$ is clear. On the other hand, if

$$a \in (\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)),$$

we can write $a = q + by^n$ for some $q \in \mathfrak{q}$, and

$$a \in \mathfrak{q} + (x) \implies ay \in \mathfrak{q} + (xy) = \mathfrak{q}.$$

So

$$by^{n+1} = ay - aq \in \mathfrak{q} \implies b \in (\mathfrak{q} : y^{n+1}) = (\mathfrak{q} : y^n).$$

By definition, this means that $by^n \in \mathfrak{q}$, and thus $a = q + by^n \in \mathfrak{q}$. This shows that $\mathfrak{q}$ is not irreducible, concluding the proof.

(2) If the set of ideals that are not a finite intersection of irreducibles were nonempty, then by Noetherianity there would be an ideal maximal with the property of not being an intersection of irreducible ideals. Such a maximal element must be an intersection of two larger ideals, each of which are finite intersections of irreducibles, giving a contradiction. □

Example 5.53. There are primary ideals that are not irreducible. For example, $(x^2, y) \cap (x, y^2) = (x^2, xy, y^2)$.

Primary decompositions, even minimal ones, are not unique.

Example 5.54. Let $R = K[x, y]$, where K is a field, and $I = (x^2, xy)$. We can write

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

These are two different minimal primary decompositions of I. To check this, we just need to see that each of the ideals (x^2, xy, y^2) and (x^2, y) are primary. Observe that each has radical $\mathfrak{m} = (x, y)$, which is maximal, so by an earlier remark, these ideals are both primary. In fact, our ideal I has infinitely many minimal primary decompositions: given any $n \geqslant 1$,

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

is a minimal primary decomposition. One thing all of these have in common is the radicals of the primary components: they are always (x) and (x, y).

In the previous example, the fact that all our minimal primary decompositions had primary components always with the same radical was not an accident. Indeed, there are some aspects of primary decompositions that are unique, and this is one of them.

Theorem 5.55 (First uniqueness theorem for primary decompositions)**.** *Suppose I is an ideal in a Noetherian ring R. Given any minimal primary decomposition of I, say*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t,$$

we have

$$\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_t}\} = \operatorname{Ass}(R/I).$$

In particular, this set is the same for all minimal primary decompositions of I.

Proof. For any primary decomposition, minimal or not, we have

$$\operatorname{Ass}(R/I) \subseteq \bigcup_i \operatorname{Ass}(R/\mathfrak{q}_i) = \{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_t}\}$$

from the lemma on intersections we proved. We just need to show that in a minimal decomposition as above, every $\mathfrak{p}_j := \sqrt{\mathfrak{q}_j}$ is an associated prime.

So fix j, and let

$$I_j = \bigcap_{i \neq j} \mathfrak{q}_i \supseteq I.$$

Since the decomposition is minimal, the module I_j/I is nonzero, hence it has an associated prime, say $\mathfrak{a}$. Since $I_j/I \subseteq R/I$, we have $\mathfrak{a} \in \operatorname{Ass}_R(R/I)$ as well. Fix $x_j \in R$ such that $\mathfrak{a}$ is the annihilator of $\overline{x_j}$ in I_j/I. Since

$$\mathfrak{q}_j x_j \subseteq \mathfrak{q}_j \cdot \bigcap_{i \neq j} \mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = I,$$

we conclude that $\mathfrak{q}_j$ is contained in the annihilator of $\overline{x_j}$, meaning $\mathfrak{q}_j \subseteq \mathfrak{a}$. Since $\mathfrak{p}_j$ is the unique minimal prime of $\mathfrak{q}_j$ and $\mathfrak{a}$ is a prime containing $\mathfrak{q}_j$, we must have $\mathfrak{p}_j \subseteq \mathfrak{a}$. On the other hand, if $r \in \mathfrak{a}$, we have $rx_j \in I \subseteq \mathfrak{q}_j$, and since $x_j \notin \mathfrak{q}_j$, we must have $r \in \mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$ by the definition of primary ideal. Thus $\mathfrak{a} \subseteq \mathfrak{p}_j$, so $\mathfrak{a} = \mathfrak{p}_j$. This shows that $\mathfrak{p}_j$ is an associated prime of R/I. □

We note that if we don't assume that R is Noetherian, we may or may not have a primary decomposition for a given ideal. It is true that if an ideal I in a general ring has a primary decomposition, then the primes occurring are the same in any minimal decomposition. However, they are not the associated primes of I in general; rather, they are the primes that occur as radicals of annihilators of elements.

There is also a partial uniqueness result for the actual primary ideals that occur in a minimal decomposition.

Theorem 5.56 (Second uniqueness theorem for primary decompositions)**.** *If I is an ideal in a Noetherian ring R, then for any minimal primary decomposition of I, say $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, the set of* minimal components *$\{\mathfrak{q}_i \mid \sqrt{\mathfrak{q}_i} \in \operatorname{Min}(R/I)\}$ is the same. Namely, $\mathfrak{q}_i = IR_{\sqrt{\mathfrak{q}_i}} \cap R$.*

Lecture of March 9, 2022

Proof. We observe that for a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ and a prime $\mathfrak{a}$

$$\operatorname{Ass}_{R_\mathfrak{a}}(R_\mathfrak{a}/\mathfrak{q}_\mathfrak{a}) = \begin{cases} \mathfrak{p}_\mathfrak{a} & \text{if } \mathfrak{p} \subseteq \mathfrak{a} \\ \varnothing & \text{if } \mathfrak{p} \not\subseteq \mathfrak{a} \end{cases}.$$

Now, since finite intersections commute with localization, then for any prime $\mathfrak{a}$,

$$I_\mathfrak{a} = (\mathfrak{q}_1)_\mathfrak{a} \cap \cdots \cap (\mathfrak{q}_t)_\mathfrak{a}$$

is a primary decomposition, although not necessarily minimal. In a minimal decomposition, choose a minimal prime $\mathfrak{a} = \mathfrak{p}_i$. Then when we localize at $\mathfrak{a}$, all the other components become the unit ideal since their radicals are not contained in $\mathfrak{p}_i$, and thus $I_{\mathfrak{p}_i} = (\mathfrak{q}_i)_{\mathfrak{p}_i}$. We can then contract to R to get $I_{\mathfrak{p}_i} \cap R = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap R = \mathfrak{q}_i$, since $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. □

Corollary 5.57. *If I has no embedded primes, then the primary decomposition of I is unique.*

Example 5.58. Let $R = \mathbb{Z}[\sqrt{-5}]$, where some elements can be written as products of irreducible elements in more than one way. For example,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We can write $(6) = (2) \cap (3)$, since 2 and 3 are comaximal. Note that

$$R/(2) \cong \frac{\mathbb{Z}[x]}{(x^2+5, 2)} \cong \frac{\mathbb{F}_2[x]}{(x^2+1)} \cong \frac{\mathbb{F}_2[x]}{(x+1)^2}.$$

Thus, this ideal has one minimal prime, given by $(x+1)$ on the right, which is $(2, 1+\sqrt{-5})$ in R. This ideal is maximal, since the quotient is isomorphic to $\mathbb{F}_2$, so (2) is $(2, 1+\sqrt{-5})$-primary. Now note that

$$R/(3) \cong \frac{\mathbb{Z}[x]}{(x^2+5, 3)} \cong \frac{\mathbb{F}_3[x]}{(x^2-1)} \cong \frac{\mathbb{F}_3[x]}{(x+1)(x-1)}.$$

The ideals $(x-1)$, $(x+1)$ are the minimal primes of the ring on the right, so $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ are the minimal primes of (3), and intersect to (3).

We conclude that

$$(6) = (2) \cap (3, 1+\sqrt{-5}) \cap (3, 1-\sqrt{-5})$$

is the unique minimal primary decomposition of (6).

Finally, we note that the primary decompositions of powers of ideals are especially interesting.

Definition 5.59 (Symbolic power)**.** If $\mathfrak{p}$ is a prime ideal in a ring R, the *nth symbolic power* of $\mathfrak{p}$ is $\mathfrak{p}^{(n)} := \mathfrak{p}^n R_{\mathfrak{p}} \cap R$.

This admits equivalent characterizations.

Proposition 5.60. *Let R be Noetherian, and $\mathfrak{p}$ a prime ideal of R.*

1. $\mathfrak{p}^{(n)} = \{r \in R \mid rs \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$.
2. $\mathfrak{p}^{(n)}$ *is the unique smallest* $\mathfrak{p}$*-primary ideal containing* $\mathfrak{p}^n$.
3. $\mathfrak{p}^{(n)}$ *is the* $\mathfrak{p}$*-primary component in any minimal primary decomposition of* $\mathfrak{p}^n$.

Proof. The first characterization follows from the definition, and the fact that expanding and contraction to/from a localization is equivalent to saturating with respect to the multiplicative set.

We know that $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary from one of the characterizations of primary. Any $\mathfrak{p}$-primary ideal satisfies $\mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$, and if $\mathfrak{q} \supseteq \mathfrak{p}^n$, then $\mathfrak{p}^{(n)} = \mathfrak{p}^n R_{\mathfrak{p}} \cap R \subseteq \mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$. Thus, $\mathfrak{p}^{(n)}$ is the unique smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$.

The last characterization follows from the second uniqueness theorem. □

In particular, note that $\mathfrak{p}^n = \mathfrak{p}^{(n)}$ if and only if $\mathfrak{p}^n$ is primary.

Example 5.61.

1. In $R = k[x, y, z]$, the prime $\mathfrak{p} = (y, z)$ satisfies $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ for all n. This follows along the same lines as above.
2. In $R = k[x, y, z] = (xy - z^n)$, where $n \geqslant 2$, we have seen that the square of $\mathfrak{p} = (y, z)$ is not primary, and therefore $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$. Indeed, $xy = z^n \in \mathfrak{p}^2$, and $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}^{(2)}$ but $y \notin \mathfrak{p}^2$.

Lecture of March 11, 2022

6. Local rings and NAK

Definition 6.1. A ring R is called a *local ring* if it has exactly one maximal ideal. We often use the notation $(R, \mathfrak{m})$ to denote R and its maximal ideal, or $(R, \mathfrak{m}, k)$ to also specify the residue field $k = R/\mathfrak{m}$. Some people reserve the term *local ring* for a Noetherian local ring, and call what we have defined a *quasilocal ring*; we will not follow this convention here.

An easy equivalent characterization is that R is local if and only if the set of nonunits of R forms an ideal: this must then be the unique maximal ideal.

The following remark is an easy source of local rings.

Remark 6.2. If R is a ring and $\mathfrak{p}$ is a prime ideal, then $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is a local ring. Indeed, the primes of $R_\mathfrak{p}$ are just the expansions of primes of R that are contained in $\mathfrak{p}$. In R, $\mathfrak{p}$ is uniquely maximal among primes contained in $\mathfrak{p}$.

Example 6.3.
(1) The ring $\mathbb{Z}/(p^n)$ is local with maximal ideal (p).
(2) The ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b \text{ when in lowest terms}\}$ is a local ring with maximal ideal (p).
(3) The ring of power series $K[\![\underline{x}]\!]$ over a field K 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 an ideal (the ideal $(\underline{x})$).
(4) The ring of complex power series holomorphic at the origin, $\mathbb{C}\{\underline{x}\}$ is local. In the above setting, one proves that the series inverse of a holomorphic function at the origin is convergent on a neighborhood of 0.
(5) A polynomial ring over a field is certainly not local; you know so many maximal ideals! A local ring we will often encounter is $K[x_1, \dots, x_d]_{(x_1,\dots,x_d)}$. 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.)
(6) Extending the following example, we have local rings like $(K[x_1, \dots, x_d]/I)_{(x_1,\dots,x_d)}$. If K is algebraically closed and I is a radical ideal, then $K[x_1, \dots, x_d]/I = K[X]$ is the coordinate ring of some affine variety, and $(x_1, \dots, x_d) = \mathfrak{m}_{\underline{0}}$ is the ideal defining the origin (as a point in $X \subseteq K^d$). Then we call $(K[x_1, \dots, x_d]/I)_{(x_1,\dots,x_d)} = K[X]_{\mathfrak{m}_{\underline{0}}}$ the *local ring of the point* $\underline{0} \in X$; some people write $\mathcal{O}_{X,\underline{0}}$. The radical ideals of this ring consist of radical ideals of $K[X]$ that are contained in $\mathfrak{m}_{\underline{0}}$, which by the Nullstellensatz correspond to subvarieties of X that contain $\underline{0}$.

There are a range of statements the go under the banner of Nakayama's Lemma a.k.a. NAK.

Proposition 6.4. *Let R be a ring, I an ideal, and M a finitely generated R-module. If $IM = M$, then*

- *there is an element $r \in 1 + I$ such that $rM = 0$, and*
- *there is an element $a \in I$ such that $am = m$ for all $m \in M$.*

Proof. Let $m_1, \dots, m_s$ be a generating set for M. By assumption, we have equations

$$m_1 = a_{11}m_1 + \cdots + a_{1s}m_s \ , \ \dots \ , \ m_s = a_{s1}m_1 + \cdots + a_{ss}m_s,$$

with $a_{ij} \in I$. Setting $A = [a_{ij}]$ and $v = [x_i]$ we have a matrix equations $Av = v$, and hence $(\mathrm{id} - A)v = 0$. By the adjoint trick, we have $\det(\mathrm{id} - A)$ kills each m_i, and hence M. Since $\det(\mathrm{id} - A) \equiv \det(\mathrm{id}) \equiv 1 \bmod I$, this determinant is the element r we seek for the first statement.

For the latter statement, set $a = 1 - r$; this is in I and satisfies $am = m - rm = m$ for all $m \in M$. □

Proposition 6.5. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module. If $M = \mathfrak{m}M$, then $M = 0$.*

Proof. By the previous lemma, there exists an element $r \in 1 + \mathfrak{m}$ that annihilates M. Such an r must be a unit, so 1 annihilates M; i.e., $M = 0$. □

Proposition 6.6. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module. For $m_1, \dots, m_s \in M$,*

$$m_1, \dots, m_s \text{ generate } M \iff \overline{m_1}, \dots, \overline{m_s} \text{ generate } M/\mathfrak{m}M.$$

Thus, any generating set for M consists of at least $\dim_k(M/\mathfrak{m}M)$ elements.

Proof. The implication $\Rightarrow$ is clear. Let $N = \langle m_1, \dots, m_s \rangle \subseteq M$. We have that $M/N = 0$ iff $M/N = \mathfrak{m}(M/N)$ iff $M = \mathfrak{m}M + N$ iff $M/\mathfrak{m}M$ is generated by the image of N. □

Definition 6.7. Let $(R, \mathfrak{m})$ be a local ring, and M a finitely generated module. A set of elements $\{m_1, \dots, m_t\}$ is a *minimal generating set* of M if the images of $m_1, \dots, m_t$ form a basis for the $R/\mathfrak{m}$ vector space $M/\mathfrak{m}M$.

Observe that any generating set for M contains a minimal generating set, and that every minimal generating set has the same cardinality.

Lemma 6.8 (Radical lemma for finitely generated ideals)**.** *If $I \subseteq J$ are ideals, $J \subseteq \sqrt{I}$ and J is finitely generated, then there is some n with $J^n \subseteq I$.*

Thus, if R is Noetherian, for every ideal I, there is some n with $\sqrt{I}^n \subseteq I$.

Proof. Write $J = (f_1, \dots, f_m)$. By definition, there are $a_1, \dots, a_m$ with $f_i^{a_i} \in I$. Let $n = a_1 + \cdots + a_m + 1$; by the pigeonhole principle, any product of at most n f_i's must lie in I.

For the second statement, just use the fact that $\sqrt{I}$ is finitely generated. □

Theorem 6.9 (Krull intersection theorem)**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = 0$.*

Proof. Let $J = \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n$. We will show that $J \subseteq \mathfrak{m}J$, hence $J = \mathfrak{m}J$, and thus $J = 0$ by NAK.

Let $\mathfrak{m}J = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ be a primary decomposition. We claim that $J \subseteq \mathfrak{q}_i$ for each i. If $\sqrt{\mathfrak{q}_i} \neq \mathfrak{m}$, pick $x \in \mathfrak{m} \smallsetminus \sqrt{\mathfrak{q}_i}$. We have $xJ \subseteq \mathfrak{m}J \subseteq \mathfrak{q}_i$, with $x \notin \sqrt{\mathfrak{q}_i}$, so $J \subseteq \mathfrak{q}_i$ by definition of primary. If instead $\sqrt{\mathfrak{q}_i} = \mathfrak{m}$, there is some N with $\mathfrak{m}^N \subseteq \mathfrak{q}_i$ by the radical lemma for finitely generated ideals. We then have $J \subseteq \mathfrak{m}^N \subseteq \mathfrak{q}_i$, and we are done. □

This result extends to modules as well.

Theorem 6.10. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, and M be a finitely generated R-module. Then $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n M = 0$.*

Proof. Consider the Nagata idealization $R \rtimes M$, which is $R \oplus M$ additively, with multiplication $(r, m)(s, n) = (rs, rn + sm)$. This is a local ring with maximal ideal $\mathfrak{m} \oplus M$: any element outside of this ideal can be written as (λ, m) with λ a unit in R, and

$$(\lambda, m)(\lambda^{-1}, -\lambda^{-2}m) = (\lambda\lambda^{-1}, \lambda(-\lambda^{-2})m + \lambda^{-1}m) = (1, 0).$$

It is a finitely generated R-module, so it is again Noetherian. We also have

$$(\mathfrak{m} \oplus M)^n = \mathfrak{m}^n \oplus \mathfrak{m}^{n-1}M.$$

If $m \in \bigcap_{n \in \mathbb{N}} \mathfrak{m}^n M$, then $(0, m) \in \bigcap_{n \in \mathbb{N}} (\mathfrak{m} \oplus M)^n = 0$, so $m = 0$. □

7. Dimension theory, globally

Lecture of March 21, 2022

7.1. **Definition of dimension.** We will now spend a while discussing the notion of dimension of a ring and dimension of a variety. To motivate the definition, let's first think in terms of varieties.

We take our inspiration from the fundamental setting of dimension theory: vector spaces. The notion of basis doesn't make sense for varieties (What does it mean to span? Where is zero?), but one relevant thing we do have for both vector spaces and for varieties is subobjects.

One way to characterize the dimension of a vector space V is the the largest number d such that there is a proper chain of subspaces

$$\{0\} = V_0 \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_d = V.$$

We can try something similar for varieties, but for a reducible variety, this isn't a very good notion. For example, for a union of m points, we can cook up a chain of m proper subvarieties by adding one more point each time, but a point should be zero-dimensional by any reasonable measure. So, if we want this approach to work, we should stick to chains of irreducible subvarieties.

Definition 7.1. The *dimension* of an affine variety X is defined as

$$\sup\{d \mid \exists \text{ a strictly decreasing chain of irreducible subvarieties of } X\colon\ X_d \supsetneqq X_{d-1} \supsetneqq \cdots \supsetneqq X_0\}.$$

Over an algebraically closed field K, this information of chains of subvarieties can be translated into information about primes in the coordinate ring: namely, a strictly increasing chain of irreducible subvarieties

$$X_d \supsetneqq X_{d-1} \supsetneqq \cdots \supsetneqq X_0$$

corresponds to strictly increasing chain of prime ideals

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$$

in the coordinate ring $K[X]$.

Definition 7.2. The *Krull dimension* (often just called dimension) of a commutative ring R, written $\dim(R)$, is defined to be

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

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

For a (proper) chain of primes

$$\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$$

its *length* is d, the number of (proper) containments in the chain; such a chain is *saturated* if for each i, there is no $\mathfrak{q} \in \operatorname{Spec}(R)$ with $\mathfrak{p}_i \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}_{i+1}$. One can equivalently define $\dim(R)$ as the supremum of the lengths of saturated chains of primes of R.

Note in the definition that the set we are taking the sup over is a subset of $\mathbb{N}$, so this sup is either ∞ if unbounded or the maximum if bounded.

Example 7.3.

(1) The dimension of a field is zero.
(2) A ring is zero-dimensional if and only if every minimal prime of R is maximal.
(3) 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

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

since there is a saturated chain of primes

$$(0) \subsetneqq (x_1) \subsetneqq (x_1, x_2) \subsetneqq \cdots \subsetneqq (x_1, \dots, x_d).$$

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

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

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

Remark 7.4. We will show eventually that $\dim(K[x_1, \dots, x_d]) = d$. The case $d = 1$ follows from above, i.e. $\dim(K[x]) = 1$, since this ring is a PID.

Remark 7.5. The definition of dimension is most meaningful for Noetherian rings, although

- There are nonNoetherian rings of finite Krull dimension: for a field K, the ring $K[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$ is not Noetherian, as
$$(x_1) \subsetneqq (x_1, x_2) \subsetneqq (x_1, x_2, x_3) \subsetneqq \cdots$$
is an infinite ascending chain, but its dimension is zero, since $\sqrt{(0)} = (x_1, x_2, \dots)$ is a maximal ideal, and hence $(x_1, x_2, \dots)$ is the unique minimal prime of R, which is also maximal.
- There are Noetherian rings of infinite dimension. This was shown in a famous example due to Nagata presented below.

Example 7.6 (Nagata)**.** Let $R = K[x_{11}, x_{21}, x_{22}, x_{31}, x_{32}, x_{33}, \dots]$ be a polynomial ring in infinitely many variables, which we are thinking of as arranged in an infinite triangle. R is clearly infinite-dimensional and not Noetherian. Let

$$W = R \smallsetminus \big((x_{11}) \cup (x_{21}, x_{22}) \cup (x_{31}, x_{32}, x_{33}) \cup \cdots\big) = \bigcap_{n \in \mathbb{N}} \big(R \smallsetminus (x_{n1}, \dots, x_{nn})\big)$$

and $S = W^{-1}R$. Note that W is an intersection of multiplicatively closed subsets, so this is a valid localization of R.

For any n, we have a chain of primes

$$(x_{n1}) \subsetneqq (x_{n1}, x_{n2}) \subsetneqq \cdots \subsetneqq (x_{n1}, \dots, x_{nn})$$

in R. As these are all contained in the last one, none of these intersects W, so the expansions yield a proper chain of primes in S. It follows that $\dim(S) \geqslant n$ for all $n \in \mathbb{N}$, so S is infinite-dimensional.

It turns out that S is Noetherian, which is not at all obvious. We skip the proof of this.

To aid in computing dimension we make the following related definition.

Definition 7.7. 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

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

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

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

To get a feel for these definitions, we make a sequence of easy observations. We use the phrase *minimal primes of* R and the notation $\operatorname{Min}(R)$ to mean $\operatorname{Min}(0)$.

Proposition 7.8 (Properties of dimension and height)**.**

(1) *A prime has height zero if and only if it is a minimal prime of R.*
(2) *An ideal has height zero if and only if it is contained in a minimal prime of R. In particular, in a domain, every nonzero ideal has positive height.*
(3) $\dim(R) = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\} = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Min}(R)\}$.
(4) $\dim(R) = \sup\{\operatorname{height}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\} = \sup\{\operatorname{height}(\mathfrak{m}) \mid \mathfrak{m} \in \operatorname{Max}(R)\}$.
(5) *If I is an ideal, then* $\dim(R/I)$ *is the supremum of the lengths of (saturated) chains of primes of R, $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$, with each $\mathfrak{p}_i \in V(I)$.*
(6) *If $\mathfrak{p}$ is prime,* $\dim(R/\mathfrak{p}) + \operatorname{height}(\mathfrak{p}) \leqslant \dim(R)$.
(7) *If I is an ideal,* $\dim(R/I) + \operatorname{height}(I) \leqslant \dim(R)$.
(8) *If W is a multiplicative set, then* $\dim(W^{-1}R) \leqslant \dim(R)$.
(9) *If $\mathfrak{p}$ is prime, then* $\operatorname{height}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$.
(10) *If $\mathfrak{p} \subseteq \mathfrak{q}$ are primes, then* $\dim(R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}})$ *is the supremum of the lengths of (saturated) chains of primes in R of the form $\mathfrak{p} = \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{q}$.*

Proof. We only discuss a few here.

For (2), if I is contained in a minimal prime $\mathfrak{q}$ of R, then there is some $\mathfrak{p} \in \operatorname{Min}(I)$ with $\mathfrak{p} \subseteq \mathfrak{q}$, so $\mathfrak{p} = \mathfrak{q}$, and $\operatorname{height}(\mathfrak{p}) = 0$ by (1), so $\operatorname{height}(I) = 0$ by definition. Conversely, if $\operatorname{height}(I) = 0$, by definition, there is a minimal prime of I of height 0, so some minimal prime of I is a minimal prime of R, so I is contained in a minimal prime of R.

For (6), it suffices to show that if $\dim(R/\mathfrak{p}) \geqslant a$ and $\operatorname{height}(\mathfrak{p}) \geqslant b$ then $\dim(R) \geqslant a + b$. By definition, $\operatorname{height}(\mathfrak{p}) \geqslant b$ means that there is a chain of primes

$$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_b = \mathfrak{p}.$$

By (5), $\dim(R/\mathfrak{p}) \geqslant a$ means that there is a chain of primes

$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_a$$

with $\mathfrak{a}_0 \supseteq \mathfrak{p}$. We can assume without loss of generality that $\mathfrak{a}_0 = \mathfrak{p}$, since if not, we can add it to the bottom of the chain. Putting these chains together, we get a chain of length $a + b$ in $\operatorname{Spec}(R)$, so $\dim(R) \geqslant a + b$.

For (7), let $\dim(R/I) \geqslant a$ and $\operatorname{height}(I) \geqslant b$. The inequality $\operatorname{height}(I) \geqslant b$ means that for every minimal prime $\mathfrak{p}$ of I, $\operatorname{height}(\mathfrak{p}) \geqslant b$. The inequality $\dim(R/I) \geqslant a$ implies that there exists a minimal prime of $\mathfrak{p}$ of I such that $\dim(R/\mathfrak{p}) \geqslant a$. For such a minimal prime as in the latter statement, using (5), we get the desired conclusion.

(8)–(10) are left for you. □

Remark 7.9. We know that in Noetherian rings, there can be arbitrarily long chains of primes: the dimension can be infinite as in Nagata's example. On the other hand, any ascending proper chain of primes is finite, as a consequence of the definition. Does this imply that every prime has finite height? It does not follow:

A priori, there could be an infinite descending chain of primes, which would then give any of the primes in the chain infinite height. (This seems strange in conjunction with the fact that in any ring, any prime contains a minimal prime, but does not contradict this.)

Another possible problem is there being two primes $\mathfrak{p} \subset \mathfrak{q}$ with for each $n \in \mathbb{N}$, a chain of primes of length n from $\mathfrak{p}$ to $\mathfrak{q}$.

However, we will show later that the height of any ideal in a Noetherian ring is finite, though only a while from now.

Lecture of March 23, 2022

Optional Exercise 7.10. Let R be a UFD. Then a nonzero ideal has height 1 if and only if it is principal.

Example 7.11. Let K be a field, and $R = K[x,y,z]/(xy,xz)$. In $K[x,y,z]$, we have $\mathrm{Min}((xy,xz)) = \{(x),(y,z)\}$, so $\mathrm{Min}(R) = \{(\bar{x}),(\bar{y},\bar{z})\}$. We then have

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

In fact, once we believe that $\dim(K[y,z]) = 2$, we will believe $\dim(R) = 2$.

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

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

In $K[x,y,z]$, we have $\mathrm{height}((xy,xz)) = \min\{\mathrm{height}(x),\mathrm{height}(y,z)\} = \min\{1,\geqslant 2\} = 1$.

Geometrically this corresponds to a union of a line and a plane. The dimension of this variety is the max of the dimensions of the irreducible components, which (should be) 2.

We want to compute a nontrivial example of dimension. We will generalize the rough outline of this example later to prove our main theorems about dimension of finitely generated algebras over fields. We note a simple fact on integral extensions to prepare.

Optional Exercise 7.12. Let $R \subseteq S$ be an integral inclusion of rings. Then for every nonzero $s \in S$, there is some $s' \in S$ such that $ss' \in R \smallsetminus 0$.

Example 7.13. Let K be an infinite field. Let $R = K[t^3,t^4,t^5]$. We have shown that $R \cong \dfrac{K[x,y,z]}{(x^3-yz,y^2-xz,z^2-x^2y)}$, and that R is the coordinate ring of the curve $X = \{(t^3,t^4,t^5) \mid t \in K\}$ over an infinite field K. As X is a curve / is parameterized by a single parameter we expect the dimension of the ring R (equivalently of the variety X) to be 1. Let's prove this.

R is a domain, so (0) is the unique minimal prime. We need to show that any nonzero prime ideal is maximal.

Set $S = K[t^3] \subseteq R$. We note that t^3 does not satisfy any algebraic relation over K, so S is isomorphic to a polynomial ring in one variable (corresponding to t^3). Furthermore, this inclusion is integral, since $(t^4)^3 - (t^3)^4 = 0$ and $(t^5)^3 - (t^3)^5 = 0$.

Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be nonzero. Note first that $\mathfrak{p} \cap S \neq 0$, since if $f \in \mathfrak{p}$, then there is some nonzero multiple of f in S by the exercise. Since $\dim(S) = 1$, $\mathfrak{p} \cap S$ is maximal. The inclusion

$$\frac{S}{\mathfrak{p}\cap S} \hookrightarrow \frac{R}{\mathfrak{p}}$$

is integral: an dependence relation for any representative yields a dependence relation. Since $\frac{S}{\mathfrak{p}\cap S}$ is a domain, $\frac{R}{\mathfrak{p}}$ is a field, and the inclusion is integral, we conclude that $\frac{S}{\mathfrak{p}\cap S}$ is a field, so $\mathfrak{p} \cap S$ is maximal.

Definition 7.14. A ring is *catenary* if for every pair of primes $\mathfrak{q} \supseteq \mathfrak{p}$ in R, every saturated chain of primes $\mathfrak{p} = \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{q}$ has the same length.
A ring is *equidimensional* if every maximal ideal has the same finite height, and every minimal prime has the same dimension.

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 gave the first example of a Noetherian noncatenary ring in the paper.

Example 7.15. Here is an example which shows that the inequality $\dim(R/I) + \text{height}(I) \leqslant \dim(R)$ can fail to be an equality.

Let $R = \mathbb{Z}_{(2)}[x]$ and consider $\mathfrak{p} = (2x-1)$. Now $\mathfrak{p}$ is a prime of height 1 and $R/\mathfrak{p} \cong \mathbb{Q}$, so $\dim(R/\mathfrak{p}) = 0$, and therefore $\dim(R/\mathfrak{p}) + \text{height}(\mathfrak{p}) = 1$ whereas $\dim R \geqslant 2$ as attested by the chain $(0) \subsetneq (2) \subsetneq (2, x)$. In fact, $\dim R = 2$, but I won't justify this.

The ring R in this example is in fact a catenary domain. Notice that there are maximal ideals of distinct heights in this ring, for example the ideal $\mathfrak{p}$ given above is a prime of height 1 whereas and another maximal ideal $\mathfrak{m} = (2, x)$ has height 2. Thus this ring is not equidimensional.

Lecture of March 25, 2022

We give a related definition of dimension for modules.

Definition 7.16. The *dimension* of an R-module M is defined as

$$\dim(M) = \dim(R/\operatorname{ann}_R(M)).$$

Optional Exercise 7.17. Show that if M is finitely generated, then $\dim(M)$ is the same as the largest length of a chain of primes in $\operatorname{Supp}_R(M)$.

7.2. **Over, up, down theorems.** In this section, we will collect theorems about the spectrum of a ring: theorems that assert that the map on Spec is surjective, and theorems about lifting chains of primes.

It will be convenient to think in terms fo fibers. For a map of topological spaces $f : X \to Y$ (or in various other categories) and $y \in Y$, the *fiber* over y is the subspace $f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$; if f is continuous and $y \in Y$ is closed, then $f^{-1}(y) \subseteq X$ is closed.

Optional Exercise 7.18. Let $\phi : X \to Y$ be a morphism of affine varieties, with $X = Z(I) \subseteq \mathbb{A}^n$ (with coordinates $x_1, \ldots, x_n$), $Y = Z(J) \subseteq \mathbb{A}^m$ (with coordinates $y_1, \ldots, y_m$), and $y = (a_1, \ldots, a_m) \in Y$. Then

$$\phi^{-1}(y) = Z(I, \phi^*(y_1 - a_1), \ldots, \phi^*(y_m - a_m)),$$

and hence

$$K[\phi^{-1}(y)] \cong \frac{K[X]}{\mathcal{I}(y)K[X]},$$

where $\mathcal{I}(y)K[X]$ denotes the expansion of the ideal $\mathcal{I}(y) \in K[Y]$ to $K[X]$ via the map ϕ^*.

Definition 7.19. Let $\psi : R \to S$ be a ring homomorphism and $\mathfrak{p} \in \operatorname{Spec}(R)$ be a prime ideal. We define the *fiber ring* of ψ over $\mathfrak{p}$ as

$$\kappa_\psi(\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S),$$

where, by abuse of notation, we write $R \smallsetminus \mathfrak{p}$ for the image of $R \smallsetminus \mathfrak{p}$ in S (and $\mathfrak{p}S$ for $\psi(\mathfrak{p})S$ as usual).

In the special case $\mathfrak{m} \subseteq R$ is maximal, $S/\mathfrak{m}S$ is an $R/\mathfrak{m}$-module, which is a vector space, so every element of $R \smallsetminus \mathfrak{m}$ acts as a unit on $S/\mathfrak{m}S$, so the localization is redundant, and

$$\kappa_\psi(\mathfrak{m}) = S/\mathfrak{m}S.$$

As another special case, for the identity map, we simply write $\kappa(\mathfrak{p})$. That is,

$$\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}.$$

The point of this definition is the following.

Lemma 7.20. *Let $\psi : R \to S$ be a ring homomorphism and $\mathfrak{p} \in \operatorname{Spec}(R)$ be a prime ideal. The natural map $S \to \kappa_\psi(\mathfrak{p})$ induces a homeomorphism (in particular, an order-preserving bijection)*

$$\operatorname{Spec}(\kappa_\psi(\mathfrak{p})) \cong \{\mathfrak{q} \in \operatorname{Spec}(S) \mid \psi^*(\mathfrak{q}) = \mathfrak{p}\},$$

where the right-hand side obtains the subspace topology from $\operatorname{Spec}(S)$.

Proof. First, we recall that for any localization map or any quotient map, the induced map on Spec is a homeomorphism onto its image. Write our natural map as $S \to S/\psi(\mathfrak{p})S \to \psi(R \smallsetminus \mathfrak{p})^{-1}(S/\psi(\mathfrak{p})S)$. Then $\mathfrak{q}$ is in the image of the induced map on Spec if and only if $\mathfrak{q} \supseteq \psi(\mathfrak{p})S$ and $\mathfrak{q} \cap \psi(R \smallsetminus \mathfrak{p}) = \varnothing$. The first condition is equivalent to $\mathfrak{q} \supseteq \psi(\mathfrak{p})$, which in turn means $\psi^{-1}(\mathfrak{q}) \supseteq \mathfrak{p}$; the latter condition is equivaalent to $\psi^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}$. Together, $\mathfrak{q}$ is in the image if and only if $\psi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

Lemma 7.21 (Image criterion)**.** *Let $\varphi : R \to S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p} \in \operatorname{im}(\varphi^*)$ if and only if $\mathfrak{p}S \cap R = \mathfrak{p}$.*

Proof. If $\mathfrak{p}S \cap R = \mathfrak{p}$, then

$$\frac{R}{\mathfrak{p}} = \frac{R}{\mathfrak{p}S \cap R} \hookrightarrow \frac{S}{\mathfrak{p}S},$$

so, localizing at $(R \smallsetminus \mathfrak{p})$, we get an injection $\kappa(\mathfrak{p}) \hookrightarrow \kappa_\varphi(\mathfrak{p})$. The latter ring is nonzero, so its spectrum is nonempty. Thus, there is a prime mapping to $\mathfrak{p}$.

If $\mathfrak{p}S \cap R \neq \mathfrak{p}$, then $\mathfrak{p}S \cap R \supsetneq \mathfrak{p}$ (the other containment always holds). Then, if $\mathfrak{q} \cap R = \mathfrak{p}$, we have $\mathfrak{q} \supseteq \mathfrak{p}S$, so $\mathfrak{q} \cap R \supsetneq \mathfrak{p}$. □

Note that $\mathfrak{p}S$ may not be prime, in general.

Example 7.22. Let $R = \mathbb{C}[x^n] \subseteq S = \mathbb{C}[x]$. The ideal $(x^n-1)R$ is prime, while $(x^n-1)S = (\prod_{i=0}^{n-1} x-\zeta^i)S$, where ζ is a primitive nth root of unity, is not. However, each of its minimal primes $(x-\zeta^i)S$ contracts to $(x^n-1)R$. Similarly, the ideal x^nR is prime, while x^nS is not radical.

Corollary 7.23. *If $R \subseteq S$ is a direct summand, then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective.*

Proof. We know that $IS \cap R = I$ for all ideals in this case. □

We want to extend the idea of the last corollary to work for all integral extensions. The key idea is encapsulated in a definition.

Definition 7.24. Let R be a ring, S an R-algebra, and I an ideal.

- An element r of R is *integral* over I if it satisfies an equation of the form
$$r^n + a_1 r^{n-1} + \cdots + a_{n-1}r + a_n = 0 \qquad \text{with } a_i \in I^i \text{ for all } i.$$
- An element of S is integral over I if the same condition holds.
- The *integral closure* of I in R is $\overline{I}$, the set of elements of R that are integral over I.
- Similarly, we write $\overline{I}^S$ for the integral closure of I in S.

We leave a little exercise for you.

Optional Exercise 7.25. Let $R \subseteq S$, I be an ideal of S, and t be an indeterminate. Consider the rings $R[It] \subseteq R[t] \subseteq S[t]$.

(1) $\overline{I}^S = \{s \in S \mid st \in S[t] \text{ is integral over the ring } R[It]\}$.
(2) $\overline{I}^S$ is an ideal.

We note that in older texts and papers (e.g., Atiyah-Macdonald and Kunz) a different definition is given for integral closure of an ideal. The one we use here is more-or-less universally accepted as the correct notion.

Lemma 7.26 (Extension-contraction lemma for integral extensions)**.** *Let $R \subseteq S$ be integral, and I be an ideal of R. Then, $IS \subseteq \overline{I}^S$. Hence, $IS \cap R \subseteq \overline{I}$.*

Proof. Let $x \in IS$. We can write $x = \sum_{i=1}^t a_i s_i$ with $a_i \in I$. Taking $S' = R[s_1, \ldots, s_t]$, we also have $x \in IS'$. Thus, it suffices to show the statements in the case S is module-finite over R.

Let $S = \sum Rb_i$. We have $xb_i = (\sum_k a_k s_k)b_i = \sum_j a_{ij} b_j$ with $a_{ij} \in I$. We can write this as a matrix-acts-like-a-scalar equation $xv = Av$, where $v = (b_1, \ldots, b_u)$, and $A = [a_{ij}]$. By the adjoint trick, we have $\det(xI - A)v = 0$. Since we can assume $b_1 = 1$, we have $\det(xI - A) = 0$. The fact that this is the type of equation we want follows from the monomial expansion of the determinant: any monomial is a product of n terms where some of the are copies of x, and the rest are elements of I.

The last statement follows from the fact that $\overline{I}^S \cap R = \overline{I}$, which is immediate from the definition. □

Lecture of March 28, 2022

If $\mathfrak{p}$ is in the image of the induced map on spec, it must be the contraction of some minimal prime of $\mathfrak{p}S$, but not necessarily every minimal prime of $\mathfrak{p}S$.

Example 7.27. Let $R = K[u, v] \xrightarrow{\alpha} S = K[x, y]$ via $\alpha(u) = x$, $\alpha(v) = xy$. Then vS has two minimal primes $(x), (y)$. Note that $(x) \cap R = (u, v)$, but $(y) \cap R = (v)$.

Theorem 7.28 (Lying over)**.** *If $R \subseteq S$ is an integral inclusion then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective.*

Proof. We observe that $\overline{I} \subseteq \sqrt{I}$. Thus, for $\mathfrak{p}$ prime, by the previous lemma, $\mathfrak{p}S \cap R = \mathfrak{p}$, and the result follows from the image criterion. □

Remark 7.29. Both "integral" and "inclusion" are important: the map $R \to R_f$ is a nonintegral inclusion if f is a nonzerodivisor, and the image is the complement of $V(f)$; the map $R \to R/(f)$ is an integral noninclusion, and the the image is $V(f)$.

Theorem 7.30 (Incomparability)**.** *If $\varphi : R \to S$ is integral, and $\mathfrak{q} \subseteq \mathfrak{q}'$ are such that $\varphi^*(\mathfrak{q}) = \varphi^*(\mathfrak{q}')$, then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Since the map $R \to R/\ker(R)$ is injective on spectra, we can replace R by the quotient and assume φ is an integral inclusion.

Now, if $R \hookrightarrow S$ is integral, then $R/\mathfrak{p} \hookrightarrow S/\mathfrak{p}S$ (which is injective by the lemma above) is integral; take an integral equation for a representative. Furthermore, localizing at $(R \smallsetminus \mathfrak{p})$ preserves integrality: if $x \in S$ and $w \in R \smallsetminus \mathfrak{p}$, then we have equations of the form

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0 \Longrightarrow (\frac{x}{w})^n + \frac{r_1}{w}(\frac{x}{w})^{n-1} + \cdots + \frac{r_n}{w^n} = 0.$$

We then have that $\kappa(\mathfrak{p}) \hookrightarrow \kappa_\varphi(\mathfrak{p})$ is integral. If $\mathfrak{q}$ is a prime of $\kappa_\varphi(\mathfrak{p})$, then $\kappa(\mathfrak{p}) \subseteq \kappa_\varphi(\mathfrak{p})/\mathfrak{q}$ is an integral inclusion from a field to a domain, and by a lemma from a while ago, we must have that $\kappa_\varphi(\mathfrak{p})/\mathfrak{q}$ is a field. Therefore, $\kappa_\varphi(\mathfrak{p})$ is zero-dimensional. Since there are no inclusions between primes in $\kappa_\varphi(\mathfrak{p})$, there are no inclusions between primes that contract to $\mathfrak{p}$. □

Corollary 7.31. *If $R \to S$ is integral, and S is Noetherian, then for any $\mathfrak{p} \in \operatorname{Spec}(R)$, only finitely many primes contract to $\mathfrak{p}$.*

Proof. For the first statement, this case the fiber ring $\kappa_\varphi(\mathfrak{p})$ of any prime is also Noetherian, hence has finitely many minimal primes. Every prime of the fiber is minimal, though. □

Optional Exercise 7.32. If $S = \sum_{i=1}^t Rs_i$ is generated as an R-module by t elements, then for any prime of R, at most t primes of S map to $\mathfrak{p}$.

Corollary 7.33. *If $R \to S$ is integral, then* $\operatorname{height}(\mathfrak{q}) \leqslant \operatorname{height}(\mathfrak{q} \cap R)$ *for any $\mathfrak{q} \in \operatorname{Spec}(S)$. In particular,* $\dim(S) \leqslant \dim(R)$.

Proof. Given a chain of primes $\mathfrak{a}_0 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n = \mathfrak{q}$ in $\operatorname{Spec}(S)$, we can contract to R, and we get a chain of distinct primes in $\operatorname{Spec}(R)$, so the height of the latter is at least as big. □

Theorem 7.34 (Going up)**.** *If $R \to S$ is integral, then for every $\mathfrak{p} \subsetneqq \mathfrak{p}'$ in* $\operatorname{Spec}(R)$ *and $\mathfrak{q}$ in* $\operatorname{Spec}(S)$ *with $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{q}' \in \operatorname{Spec}(S)$ with $\mathfrak{q} \subsetneqq \mathfrak{q}'$ and $\mathfrak{q}' \cap R = \mathfrak{p}'$.*

Proof. Consider the map $R/\mathfrak{p} \to S/\mathfrak{q}$. This is integral, as we observed above. It is also injective, so lying over applies. Thus, there is a prime $\mathfrak{a}$ of $S/\mathfrak{q}$ that contracts to the prime $\mathfrak{p}'/\mathfrak{p}$ in $\operatorname{Spec}(R/\mathfrak{p})$. We can write $\mathfrak{a} = \mathfrak{q}'/\mathfrak{q}$ for some $\mathfrak{q}' \in \operatorname{Spec}(S)$, and we must have that $\mathfrak{q}'$ contracts to $\mathfrak{p}'$. □

Corollary 7.35. *If $R \subseteq S$ is integral, then* $\dim(R) = \dim(S)$.

Proof. We just need to show that $\dim(R) \leqslant \dim(S)$. Given a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ in $\operatorname{Spec}(R)$, by lying over, there is a prime $\mathfrak{q}_0 \in \operatorname{Spec}(S)$ contracting to $\mathfrak{p}_0$. Then by going up, we have $\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1$ with $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Continuing, we can build a chain of distinct primes in S of length n. □

Lecture of March 30, 2022

We have now established almost everything we might have hoped to be true about dimension for integral extensions. The only remaining issue is whether heights of primes are preserved.

Definition 7.36. A domain is *normal* if it is integrally closed in its field of fractions.

Lemma 7.37. *A unique factorization domain is normal: in particular, a polynomial ring over a field is normal.*

Proof. Let R be a UFD, and $r/s \in \operatorname{frac}(R)$ be integral over R. We can assume that r and s have no common factor. Then we have for some a_i's in R

$$\frac{r^n}{s^n} + a_1 \frac{r^{n-1}}{s^{n-1}} + \cdots + a_n = 0 \quad \Rightarrow \quad r^n = -(a_1 r^{n-1} s + \cdots + a_n s^n).$$

Any irreducible factor of s must then divide r^n, and hence divide r; if s is not a unit then this contradicts that there is no common factor. Thus, $r/s \in R$. □

Lemma 7.38. *Let R be a normal domain, x be an element integral over R in some larger domain. Let K be the fraction field of R, and $f(t) \in K[t]$ be the minimal polynomial of x over K.*

1. *If x is integral over R, then $f(t) \in R[t] \subseteq K[t]$.*
2. *If x is integral over a prime $\mathfrak{p}$, then $f(t)$ has all of its nonleading coefficients in $\mathfrak{p}$.*

Proof. Let x be integral over R. Fix an algebraic closure of K containing x, and let $x_1 = x, x_2, \dots, x_u$ be the roots of f. Since $f(t)$ divides a monic equation for x, each x_i is integral over R.

Let $S = R[x_1, \dots, x_u] \subseteq \overline{K}$. This is a module-finite extension of R, so all of its elements are integral over R. The coefficients of $f(t)$ are elementary symmetric polynomials in the x's, hence they lie in S. But, $S \cap K = R$ since R is normal. Thus, the first statement holds.

Now, let x be integral over $\mathfrak{p}$. All of the x's are integral over $\mathfrak{p}$ by the same argument as above. Since each $x_j \in \overline{\mathfrak{p}}^S$, any elementary symmetric polynomial in the x's lies in $\overline{\mathfrak{p}}^S$. Thus, the nonleading coefficients lie in $\overline{\mathfrak{p}}^S \cap R = \mathfrak{p}$. □

Theorem 7.39 (Going down)**.** *Suppose that R is a normal domain, S is a domain, and $R \subseteq S$ is integral. Then, for every $\mathfrak{p}' \subsetneq \mathfrak{p}$ in $\operatorname{Spec}(R)$ and $\mathfrak{q}$ in $\operatorname{Spec}(S)$ with $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{q}' \in \operatorname{Spec}(S)$ with $\mathfrak{q}' \subsetneq \mathfrak{q}$ and $\mathfrak{q}' \cap R = \mathfrak{p}'$. In a picture:*

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

Proof. Let $W = (S \smallsetminus \mathfrak{q})(R \smallsetminus \mathfrak{p}')$ be the multiplicative set consisting of products of elements in $S \smallsetminus \mathfrak{q}$ and $R \smallsetminus \mathfrak{p}'$. Note that each of these sets contains 1, so each set is in the product. We want to show that $W \cap \mathfrak{p}'S$ is empty. It will follow that $W^{-1}(S/\mathfrak{p}'S) = (S \smallsetminus \mathfrak{q})^{-1}\kappa_S(\mathfrak{p}')$ has a prime ideal, and hence there is a prime of S contained in $\mathfrak{q}$ contracting to $\mathfrak{p}'$.

To that end, suppose $x \in \mathfrak{p}'S \cap W$. Since $x \in \mathfrak{p}'S$, it is integral over $\mathfrak{p}'$, so write $x = rs$ with $r \in R \smallsetminus \mathfrak{p}', s \in S \smallsetminus \mathfrak{q}$, and consider the minimal polynomial of x over $\operatorname{frac}(R)$:

$$h(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

By the lemma above, each $a_i \in \mathfrak{p}' \subseteq R$. Then, since $r \in K$, substituting $x = rs$ yields and dividing by r^n yields a polynomial that, viewed as a polynomial in s, is irreducible. That is, the minimal polynomial of s is

$$g(s) = s^n + \frac{a_1}{r}s^{n-1} + \cdots + \frac{a_n}{r^n} = 0.$$

Since $s \in S$, hence is integral over R, the lemma above says that each $\frac{a_i}{r^i} =: v_i \in R$. Since $r \notin \mathfrak{p}'$, and $r^i v_i = a_i \in \mathfrak{p}'$, we have $v_i \in \mathfrak{p}'$, and the equation $g(s) = 0$ then shows that $s \in \sqrt{\mathfrak{p}'S}$. Since $\mathfrak{q} \in \operatorname{Spec}(S)$ contains $\mathfrak{p}S$ and hence $\mathfrak{p}'S$, we have $s \in \sqrt{\mathfrak{p}'S} \subseteq \mathfrak{q}$. This is the desired contradiction. □

Corollary 7.40. *If R is a normal domain, S is a domain, and $R \subseteq S$ is integral, then* $\operatorname{height}(\mathfrak{q}) = \operatorname{height}(\mathfrak{q} \cap R)$ *for any $\mathfrak{q} \in \operatorname{Spec}(S)$.*

Proof. We already know that $\operatorname{height}(\mathfrak{q}) \leqslant \operatorname{height}(\mathfrak{q} \cap R)$. Now, take a maximal chain up to $\mathfrak{q} \cap R$, and apply going down to get a chain just as long that goes up to $\mathfrak{q}$. □

Lecture of April 1, 2022

7.3. Noether normalization and dimension of affine rings.

Lemma 7.41 (Making a pure-power leading term)**.** *Let A be a domain, and $f \in R = A[x_1, \dots, x_n]$ be a (not necessarily homogeneous) polynomial of degree at most 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 $A[x_1, \dots, x_{n-1}]$, has leading term dx_n^a for some $d \in A$, $a \in \mathbb{N}$.*

Proof. The map ϕ sends a monomial term $dx_1^{a_1}\cdots x_n^{a_n}$ to a polynomial with unique highest degree term $dx_n^{a_1N^{n-1}+a_2N^{n-2}+\cdots+a_{n-1}N+a_n}$. Since each a_i is less than N in each monomial, the map $(a_1,\ldots,a_n)\mapsto a_1N^{n-1}+a_2N^{n-2}+\cdots+a_{n-1}N+a_n$ 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 7.42 (Noether Normalization)**.** *Let A be a domain, and R be a finitely generated A-algebra. Then, there is some nonzero $a\in A$ and $x_1,\ldots,x_t\in R$ algebraically independent over A such that R_a is module-finite over $A_a[x_1,\ldots,x_t]$. In particular, if $A=K$ is a field, then R is module-finite over $K[x_1,\ldots,x_t]$.*

Proof. We proceed by induction on the number of generators n of R over A, with the case $n=0$ trivial.

Now, suppose that we know the result for A-algebras generated by at most $n-1$ elements. If $R=A[r_1,\ldots,r_n]$, with $r_1,\ldots,r_n$ algebraically independent over A, we are done. Assume that there is some relation on the r's: there is some $f(x_1,\ldots,x_n)\in A[x_1,\ldots,x_n]$ such that $f(r_1,\ldots,r_n)=0$. By taking an A-algebra automorphism (changing our generators), we can assume that f has leading term ax_n^N (in terms of x_n) for some a. Then, f is monic in x_n after inverting a, so R_a is module-finite over $A_a[r_1',\ldots,r_{n-1}']$. By hypothesis, $A_{ab}[r_1',\ldots,r_{n-1}']$ is module-finite over $A_{ab}[r_1'',\ldots,r_s'']$ for some $b\in A$ and $r_1'',\ldots,r_s''$ that are algebraically independent over A. Since R_{ab} is module-finite over $A_{ab}[r_1',\ldots,r_{n-1}']$, we are done.

□

Theorem 7.43. *Let R be a finitely generated domain over a field K. Let $K[z_1,\ldots,z_d]$ be any Noether normalization for R. Then, for any maximal ideal $\mathfrak{m}$ of R, the length of any saturated chain of primes from 0 to $\mathfrak{m}$ is d. In particular, the dimension of R is d.*

Proof. We prove by induction on d that for any finitely generated domain with a Noether normalization with d algebraically independent elements, any saturated chain of primes ending in a maximal ideal has length d.

When $d=0$, R is a domain that is integral over a field, hence is a field, so the statement follows trivially.

Pick a saturated chain

$$0\subsetneq\mathfrak{q}_1\subsetneq\cdots\subsetneq\mathfrak{q}_k=\mathfrak{m}$$

and consider the contractions to $A=K[z_1,\ldots,z_d]$:

$$0\subsetneq\mathfrak{p}_1\subsetneq\cdots\subsetneq\mathfrak{p}_k.$$

By the saturated condition, $\mathfrak{q}_1$ has height 1, and so does $\mathfrak{p}_1$, since we have a module-finite inclusion of a normal domain into a domain. Since A is a UFD, $\mathfrak{p}_1=(f)$ for some prime element f. After a change of variables, we can assume that f is monic in z_d over $K[z_1,\ldots,z_{d-1}]$. Then,

$$0=\mathfrak{q}_1/\mathfrak{q}_1\subsetneq\mathfrak{q}_2/\mathfrak{q}_1\subsetneq\cdots\subsetneq\mathfrak{q}_k/\mathfrak{q}_1=\mathfrak{m}/\mathfrak{q}_1$$

is a saturated chain in the affine domain $R/\mathfrak{q}_1$ to the maximal ideal $\mathfrak{m}/\mathfrak{q}_1$. Now, $K[z_1,\ldots,z_{d-1}]\subseteq A/(f)\subseteq R/\mathfrak{q}_1$ are module-finite, and we can apply the induction hypothesis to say that the chain we found in $R/\mathfrak{q}_1$ has length $d-1$, so $k-1=d-1$, and $k=d$.

□

Corollary 7.44. *The dimension of the polynomial ring $K[x_1,\ldots,x_d]$ is d.*

Corollary 7.45. *If R is a K-algebra, the dimension of R is less than or equal to the minimal size of a generating set for R. If equality holds for some finite generating set, then R is isomorphic to a polynomial ring over K, and the generators are algebraically independent.*

Proof. The first statement is trivial unless R is finitely generated, in which case we can write $R = K[f_1, \dots, f_s] \cong K[x_1, \dots, x_s]/I$ for some ideal I. We have $\dim(R) \leqslant s$, for certain. If $I \neq 0$, then $\dim(R) < s$, since the zero ideal is not contained in I. □

Lecture of April 4, 2022

Corollary 7.46. *Let R be a finitely generated algebra over a field.*

- *R is catenary.*

If additionally R is a domain, then

- *R is equidimensional, and*
- $\operatorname{height}(I) = \dim(R) - \dim(R/I)$ *for all ideals I.*

Proof. Let $\mathfrak{p} \subseteq \mathfrak{q}$ be primes in R. We can quotient out by $\mathfrak{p}$, and assume that R is a domain and $\mathfrak{p} = 0$. Fix a saturated chain C from $\mathfrak{q}$ to a maximal ideal $\mathfrak{m}$. Given two saturated chains C', C'' from 0 to $\mathfrak{q}$, the concatenations $C'|C$ and $C''|C$ are saturated chains from 0 to $\mathfrak{m}$, and hence must have the same length. It follows that C' and C'' have the same length.

Equidimensionality is clear from the theorem.

We have $\operatorname{height}(I) = \min\{\operatorname{height}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Min}(I)\}$ and $\dim(R/I) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Min}(I)\}$. Thus, it suffices to show the equality for prime ideals. Now, take a saturated chain of primes C from 0 to $\mathfrak{p}$, and a saturated chain C' from $\mathfrak{p}$ to a maximal ideal $\mathfrak{m}$. C has length $\operatorname{height}(\mathfrak{p})$ by catenarity and definition of height, C' has length $\dim(R/\mathfrak{p})$ by the theorem, and $C|C'$ has length $\dim(R)$ by the theorem. □

Recall that the *transcendence degree* of a field extension is the size of a transcendence basis.

Corollary 7.47. *If R is a finitely generated domain over a field K, then* $\dim(R) = \operatorname{trdeg}_K(\operatorname{frac}(R))$.

Proof. If $R \subseteq S$ is module-finite, then $\operatorname{frac}(R) \subseteq \operatorname{frac}(S)$ is algebraic, and hence they have the same transcendence degree over K. In particular, if $A = K[z_1, \dots, z_d]$ is a Noether normalization for R,

$$\operatorname{trdeg}_K(\operatorname{frac}(R)) = \operatorname{trdeg}_K(\operatorname{frac}(A)) = \operatorname{trdeg}_K(K(z_1, \dots, z_d)) = d = \dim(A) = \dim(R). \qquad \square$$

Example 7.48. Let $R = K[xu, xv, yu, yv] \subseteq K[x, y, u, v]$, where K is a field and x, y, u, v are indeterminates. Then

$$\operatorname{frac}(R) = K(xu, xv, yu, yv) = K(xu, v/u, y/x, yv/xu) = K(xu, v/u, y/x),$$

and these last three are algebraically independent over K. Thus, $\dim(R) = 3$.

Example 7.49. Let $R = \dfrac{K[x, y, z]}{(xy, xz)}$, where K is a field and x, y, z are indeterminates. We can compute $\dim(R)$ by going modulo the minimal primes of R and taking the maximum of the dimensions:

$$\dim(R) = \max\{\dim(K[x]), \dim(K[y, z])\} = 2.$$

Alternatively, we can find a Noether normalization: namely $A = K[x - y, x - z]$ works. Then R is integral over A, as it is generated as an algebra over A by x, and $x^2 + x(y - x) = xy = 0$ in R gives an integral dependence equation.

Note that $K[x, y] \subseteq R$ is not a Noether normalization, since $xy = 0$ in R, and neither is $K[y, z]$ since x is not integral over this ring.

Example 7.50. Let us compute the dimension of the ring $R = K[a, b, c, d]/I$, where

$$I = (b^2 - ac, c^2 - bd, bc - ad).$$

We claim that $A = K[a, d] \subseteq R$ is a Noether normalization. The inclusion is integral, since $b^2 = ac$ implies $b^4 = a^2c^2 = abd$, so b satisfies $t^4 - adt = 0$; similarly with c. We also need to show that a, d are algebraically independent over K, or equivalently that the map from the polynomial ring $\psi : K[u, v] \to R$ with $\psi(u) = a$, $\psi(v) = d$ is injective.

First assume that $K = \overline{K}$ is algebraically closed. Observe that the map

$$\begin{aligned} Z(I) &\xrightarrow{\phi} \mathbb{A}^2 \\ (a, b, c, d) &\longmapsto (a, d) \end{aligned}$$

is surjective: given $a, d \in K$, write $a = \alpha^3, d = \delta^3$, and note that $(\alpha^3, \alpha^2\delta, \alpha\delta^2, \delta^3)$ is an element of $X = \mathcal{Z}(I)$ that maps to (a, d). Thus, the kernel of the induced map on coordinate rings $K[\mathbb{A}^2] \to K[X]$ is $\mathcal{I}(\mathbb{A}^2) = 0$; i.e, the map is injective. by the Nullstellensatz, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$, and our induced map on coordinate rings is the map

$$K[u, v] \longrightarrow K[a, b, c, d]/\sqrt{I} \qquad \phi^*(u) = a,\ \phi^*(v) = d.$$

Since this map is injective, and this factors as

$$K[u, v] \xrightarrow{\psi} K[a, b, c, d]/I \twoheadrightarrow K[a, b, c, d]/\sqrt{I}$$

the first map is injective. This covers the case K is algebraically closed.

For a general field K, let J be the kernel so that

$$0 \longrightarrow J \longrightarrow K[u, v] \longrightarrow K[a, b, c, d]/I$$

is exact. Then, since $\overline{K}$ is a flat K-module, tensoring yields an exact sequence

$$0 \longrightarrow J \otimes_K \overline{K} \longrightarrow \overline{K}[u, v] \longrightarrow \overline{K}[a, b, c, d]/I,$$

so we must have $J \otimes_K \overline{K} = 0$, which implies $J = 0$, since the tensor product of two nonzero vector spaces is nonzero.

Lecture of April 6, 2022

8. Dimension theory, locally

8.1. **Dimension zero.** To prepare for our next big theorems in dimension theory, we need to understand the structure of zero-dimensional Noetherian rings. To get started on that, we will take a theorem on primary decomposition for certain ideals in not necessarily Noetherian rings.

Theorem 8.1. *Let R be a ring, not necessarily Noetherian. Let I be an ideal such that $V(I)$ is a finite set of maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_t$. Then, there is a primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ and we also have $I = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, 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 $\mathfrak{m}_iR_{\mathfrak{m}_i}$-primary, since $\operatorname{Min}(IR_{\mathfrak{m}_i}) = \{\mathfrak{m}_iR_{\mathfrak{m}_i}\}$, so $\sqrt{IR_{\mathfrak{m}_i}} = \mathfrak{m}_iR_{\mathfrak{m}_i}$, which is maximal, so $IR_{\mathfrak{m}_i}$ is primary. Then, the contraction of a primary ideal is primary so $\mathfrak{q}_i = IR_{\mathfrak{m}_i} \cap R$ is $\mathfrak{m}_i$-primary, and $I \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$. On the other hand, equality of these modules is a local property; if $\mathfrak{p} \notin V(I)$, then

$$(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t)R_{\mathfrak{p}} = \mathfrak{q}_1R_{\mathfrak{p}} \cap \cdots \cap \mathfrak{q}_tR_{\mathfrak{p}} = R_{\mathfrak{p}} \cap \cdots \cap R_{\mathfrak{p}} = R_{\mathfrak{p}} = IR_{\mathfrak{p}},$$

and if $\mathfrak{m}_i \in V(I)$

$$(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t)R_{\mathfrak{m}_i} = \mathfrak{q}_1R_{\mathfrak{m}_i} \cap \cdots \cap \mathfrak{q}_tR_{\mathfrak{m}_i} = R_{\mathfrak{m}_1} \cap \cdots \cap \mathfrak{q}_iR_{\mathfrak{m}_i} \cap \cdots \cap R_{\mathfrak{m}_i} = \mathfrak{q}_iR_{\mathfrak{m}_i} = (IR_{\mathfrak{m}_i} \cap R)R_{\mathfrak{m}_i} = IR_{\mathfrak{m}_i}.$$

The fact that this intersection is a product and the quotient ring is a direct product follows from the Chinese remainder theorem: $V(\mathfrak{q}_i + \mathfrak{q}_j) = V(\mathfrak{q}_i) \cap V(\mathfrak{q}_j) = \varnothing$, so each pair of ideals is comaximal. □

Remark 8.2. Note that for a vector space, Noetherian, Artinian, and finite-dimensional are all equivalent. Finite-dimensional implies finite length, which implies both Artinian and Noetherian. Conversely, any infinite-dimensional vector space has a sequence of linearly independent vectors $\{v_1, v_2, \dots\}$, and we can form an ascending chain of subspaces and a descending chain

$$\langle v_1 \rangle \subsetneqq \langle v_1, v_2 \rangle \subsetneqq \cdots \qquad\qquad \langle v_1, v_2, v_3, \dots \rangle \supsetneqq \langle v_2, v_3, \dots \rangle \supsetneqq \cdots .$$

Theorem 8.3. *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.*

Proof. (1)⇒(2): Since R is Noetherian of dimension zero, every prime is maximal and minimal, and there are thus finitely many. By the theorem from above, R decomposes as a direct product local rings, which are all quotients of R, so must all be Noetherian and all must have dimension zero.

(2)⇒(3): It suffices to deal with the case $(R, \mathfrak{m})$ is local. In this case, the maximal ideal is the unique minimal prime, so it consists of the nilpotents in R: $\mathfrak{m} = \sqrt{(0)}$. Since R is Noetherian, the previous lemma yields $\mathfrak{m}^n = 0$ for some n. If $\mathfrak{m} = (f_1, \dots, f_t)$, 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): This follows from earlier results on finite length modules.

(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 the decomposition theorem from earlier 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.

Lecture of April 8, 2022

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 $\mathfrak{m}$. The Artinian property guarantees a minimal element; 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 is a finite-dimensional vector space, hence of finite length. Thus, R has finite length, so ideals in R satisfy ACC, as required. □

8.2. **Height and number of generators.**

Theorem 8.4 (Krull's principal ideal theorem)**.** *Let R be a Noetherian ring, and $f \in R$. Then, every minimal prime of (f) has height at most one.*

Proof. If the theorem is false, so that there is some R, $\mathfrak{p}$, f with $\mathfrak{p}$ minimal over (f) and $\text{height}(\mathfrak{p}) > 1$, localize at $\mathfrak{p}$ and mod out by a minimal prime to obtain a Noetherian local domain $(R, \mathfrak{m})$ of dimension at least two in which $\mathfrak{m}$ is the unique minimal prime of (f). In particular, $\overline{R} = R/(f)$ is zero-dimensional. Let $\mathfrak{q}$ be a prime in between (0) and $\mathfrak{m}$.

Consider the symbolic powers $\mathfrak{q}^{(n)}$ of $\mathfrak{q}$. Our goal is to show that these stabilize in R. Since $R/(f)$ is Artinian, the descending chain of ideals

$$\mathfrak{q}\overline{R} \supseteq \mathfrak{q}^{(2)}\overline{R} \supseteq \mathfrak{q}^{(3)}\overline{R} \supseteq \cdots$$

stabilizes. We then have, for some n and all $m > n$, that $\mathfrak{q}^{(n)}\overline{R} \subseteq \mathfrak{q}^{(m)}\overline{R}$. Pulling back to R, $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(m)} + (f)$. For $q \in \mathfrak{q}^{(n)}$, write $q = q' + fr$, with $q' \in \mathfrak{q}^{(m)} \subseteq \mathfrak{q}^{(n)}$, so that $fr \in \mathfrak{q}^{(n)}$. Since $f \notin \mathfrak{q}$, $r \in \mathfrak{q}^{(n)}$. This yields $\mathfrak{q}^{(n)} = \mathfrak{q}^{(m)} + f\mathfrak{q}^{(n)}$. Thus, $\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)} = f(\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)})$, so $\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)} = \mathfrak{m}(\mathfrak{q}^{(n)}/\mathfrak{q}^{(m)})$, and by NAK, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ in R.

Now, if $a \in \mathfrak{q}$ is nonzero, we have $a^n \in \mathfrak{q}^n \subseteq \mathfrak{q}^{(n)} = \mathfrak{q}^{(m)}$ for all m, so $\bigcap_{m\in\mathbb{N}} \mathfrak{q}^{(m)} \neq 0$. On the other hand, $\mathfrak{q}^{(m)} \subseteq \mathfrak{q}^m R_{\mathfrak{q}}$, and $\bigcap_{m\in\mathbb{N}} \mathfrak{q}^{(m)} \subseteq \bigcap_{m\in\mathbb{N}} \mathfrak{q}^m R_{\mathfrak{q}} = 0$ by Krull intersection. This is the contradiction we seek. □

Remark 8.5. We note that this is stronger than the statement that the height of (f) is at most one: we recall that that only means that some minimal prime of (f) has height at most one.

Example 8.6. Noetherian is necessary. Let $R = K[x, xy, xy^2, \dots] \subseteq K[x, y]$. Note that (x) is not prime: for $a > 0$, $xy^a \notin (x)$, since $y^a \notin R$, but $(xy^a)^2 = x \cdot xy^{2a} \in (x)$. Thus, $\mathfrak{m} = (x, xy, xy^2, \dots) \subseteq \sqrt{(x)}$, and since $\mathfrak{m}$ is a maximal ideal, we have equality, so $\text{Min}\,(x) = \{\mathfrak{m}\}$. However, the ideal $\mathfrak{p} = (xy, xy^2, xy^3, \dots) = (y)K[x, y] \cap R$ is prime, and the chain $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$ shows that $\text{height}(\mathfrak{m}) > 1$.

We want to generalize this, but it is not so straightforward to run an induction. We will need a lemma that allows us to control the chains of primes we get.

Lemma 8.7. *Let R be Noetherian, $\mathfrak{p} \subsetneq \mathfrak{q} \subsetneq \mathfrak{r}$ be primes, and $f \in \mathfrak{r}$. Then there is some $\mathfrak{q}'$ with $\mathfrak{p} \subsetneq \mathfrak{q}' \subsetneq \mathfrak{r}$ and $f \in \mathfrak{q}'$.*

Proof. We can quotient out by $\mathfrak{p}$ and localize at $\mathfrak{r}$, and assume that $\mathfrak{r}$ is the maximal ideal, and that f is nonzero (for otherwise we are done); once we have succeeded in this case, we can pull back our prime to R. Then, by the principal ideal theorem, minimal primes of (f) have height one, hence are not $\mathfrak{r}$; we can take $\mathfrak{q}'$ to be one of those. □

Theorem 8.8 (Krull height theorem)**.** *Let R be a Noetherian ring, and $I = (f_1, \dots, f_n)$ be an ideal generated by n elements. Then every minimal prime of I has height at most n.*

Proof. We proceed by induction on n. The case $n = 1$ is the principal ideal theorem.

Let $I = (f_1, \dots, f_n)$ be an ideal, $\mathfrak{p}$ be a minimal prime of I, and $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h = \mathfrak{p}$ be a saturated chain of length h ending at $\mathfrak{p}$. If $f_1 \in \mathfrak{p}_1$, then we can apply the induction hypothesis to the ring $\overline{R} = R/(f_1)$ and the ideal $(f_2, \dots, f_n)\overline{R}$: the chain $\mathfrak{p}_1\overline{R} \subsetneqq \cdots \subsetneqq \mathfrak{p}_h\overline{R}$ has length $h - 1$ at most $n - 1$, so $h \leqslant n$. We use the previous lemma to replace our given chain with a chain of the same length that satisfies this hypothesis.

In the given chain, let $f_1 \in \mathfrak{p}_{i+1} \smallsetminus \mathfrak{p}_i$. If whenever $i > 0$ we can decrease i, we can eventually get to the chain we want. To do this, we just need to apply the previous lemma with $\mathfrak{r} = \mathfrak{p}_{i+1}$, $\mathfrak{q} = \mathfrak{p}_i$, and $\mathfrak{p} = \mathfrak{p}_{i-1}$. □

Lecture of April 11, 2022

Example 8.9. (1) The bound is certainly sharp: an ideal generated by n variables $(x_1, x_2, \dots, x_n)$ in a polynomial ring has height n. There are many other such ideals, like $(u^3 - xyz, x^2 + 2xz - 6y^5, vx + 7vy) \in K[u, v, w, x, y, z]$. An ideal of height n generated by n elements is called a *complete intersection*.

(2) The ideal (xy, xz) in $K[x, y, z]$ has minimal primes of heights 1 and 2.

(3) It is possible to have associated primes of height greater than the number of generators. For a cheap example, in $R = K[x, y]/(x^2, xy)$, the ideal generated by zero elements (the zero ideal) has an associated prime of height one, namely (x, y).

(4) For the same phenomenon, but in a nice polynomial ring, $I = (x^3, y^3, x^2u + xyv + y^2w) \subset R = K[u, v, w, x, y]$. Note that $x^2y^2 \notin (x^3, y^3, u, v, w) \supseteq I$, so $x^2y^2 \notin I$. On the other hand, we have

$$\begin{aligned} x(x^2y^2) &= y^2x^3 \in I \\ y(x^2y^2) &= x^2y^3 \in I \\ u(x^2y^2) &= y^2ux^2 = -y^2(xyv + y^2w) \in I \\ v(x^2y^2) &= xyvxy = -xy(x^2u + y^2w) \in I \\ w(x^2y^2) &= x^2wy^2 = -x^2(x^2u + xyv) \in I, \end{aligned}$$

so the maximal ideal of height five (u, v, w, x, y) is associated to I.

Corollary 8.10. *Let R be a Noetherian ring.*

(1) *Any ideal has finite height.*

(2) *The poset* $\operatorname{Spec}(R)$ *satisfies DCC.*

If $(R, \mathfrak{m}, k)$ is also local, then

(3) $\dim(R) \leqslant \dim_k(\mathfrak{m}/\mathfrak{m}^2) < \infty$.

Proof. (1) This is clear from Krull height since every ideal is finitely generated.

(2) Given a descending chain, the first element has finite height, so there can only be finitely many proper inclusions in such a chain.

(3) By NAK, $\mathfrak{m}$ is generated by $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ elements, so $\dim(R) = \operatorname{height}(m) \leqslant \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. □

8.3. **Systems of parameters.** Here is a sort of converse to the Krull height theorem.

Theorem 8.11. *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d. There there exist $x_1, \dots, x_d \in \mathfrak{m}$ such that $\mathfrak{m} = \sqrt{(x_1, \dots, x_d)}$.*

Proof. If $\dim(R) = 0$, this is clear, since $\mathfrak{m} = \sqrt{(0)}$.

In general, we show that we can choose $x_1, \dots, x_i \in \mathfrak{m}$ inductively such that every minimal prime of $J_i = (x_1, \dots, x_i)$ has height i, with the case $i = 0$ clear. Say that we have chosen the first i elements. If $i < d$, note $\mathfrak{m}$ is not a minimal prime of J_i, as this would contradict the Krull height theorem. Thus, by prime avoidance, we can choose $x_{i+1} \in \mathfrak{m}$ not in any minimal prime of J_i. Then every minimal prime of $J_{i+1} = J_i + (x_{i+1})$ has height at most $i+1$; on the other hand, any $\mathfrak{q} \in \operatorname{Min}(J_{i+1})$ contains some $\mathfrak{p} \in \operatorname{Min}(J_i)$ and we must have $\mathfrak{q} \supsetneq \mathfrak{p}$, since $x_{i+1} \in \mathfrak{q} \smallsetminus \mathfrak{p}$. Since $\mathfrak{p}$ has height i, $\mathfrak{q}$ must have height at least $i+1$, so exactly $i+1$, completing the induction.

Then every minimal prime of J_d has height d, its unique minimal prime must be $\mathfrak{m}$. It follows that $\sqrt{J_d} = \mathfrak{m}$. □

Corollary 8.12. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then,*

$$\dim(R) = \min\{n \mid \exists f_1, \dots, f_n : \sqrt{(f_1, \dots, f_n)} = \mathfrak{m}\}.$$

Proof. The dimension of a local ring is the height of its maximal ideal. Thus, by Krull height, the minimum n in the middle is at least $\dim(R)$, and the previous theorem gives the other direction. □

Compare the last inequality to the fact that, for an algebra over a field, the dimension is bounded by the number of generators as a K-algebra. We also want to compare this with the characterization of the dimension of a vector space as the least number of linear equations needed to cut out the origin.

Definition 8.13. A sequence of d elements $x_1, \dots, x_d$ in a d-dimensional Noetherian local ring $(R, \mathfrak{m})$ is a *system of parameters* or *SOP* if $\sqrt{(x_1, \dots, x_d)} = \mathfrak{m}$.

We say that elements $x_1, \dots, x_t$ are *parameters* if they are part of a system of parameters; this is a property of the set, not just the elements.

By the previous corollary, every local (or graded) ring admits a system of parameters, and these can be useful in characterizing the dimension of a local Noetherian ring, or the height of a prime in a Noetherian ring. To help characterize systems of parameters, we pose the following definition:

Definition 8.14. Let R be a Noetherian ring. A prime $\mathfrak{p}$ of R is *absolutely minimal* if $\dim(R) = \dim(R/\mathfrak{p})$.

Observe that an absolutely minimal prime is minimal, since $\dim(R) \geqslant \dim(R/\mathfrak{p}) + \operatorname{height}(\mathfrak{p})$.

Theorem 8.15. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $x_1, \dots, x_t \in \mathfrak{m}$.*

1. $\dim(R/(x_1, \dots, x_t)) \geqslant \dim(R) - t$.
2. *$x_1, \dots, x_t$ are parameters if and only if* $\dim(R/(x_1, \dots, x_t)) = \dim(R) - t$.
3. *$x_1, \dots, x_t$ are parameters if and only if x_1 is not in any absolutely minimal prime of R and x_i is not contained in any absolutely minimal prime of $R/(x_1, \dots, x_{i-1})$ for each $i = 2, \dots, t$.*

Proof. (1) If $\dim(R/(x_1, \dots, x_t)) = s$, then take a system of parameters $y_1, \dots, y_s$ for $R/(x_1, \dots, x_t)$, and pull back to R to get $x_1, \dots, x_t, y_1', \dots, y_s'$ in R such that the quotient of R modulo the ideal generated by these elements has dimension zero. By Krull height, we get that $t + s \geqslant \dim(R)$.

(2) Let $d = \dim(R)$. Suppose first that $\dim(R/(x_1, \dots, x_t)) = d - t$. Then, there is a SOP $y_1, \dots, y_{d-t}$ for $R/(x_1, \dots, x_t)$; lift back to R to get a sequence of d elements $x_1, \dots, x_t, y_1, \dots, y_{d-t}$ that generate an $\mathfrak{m}$-primary ideal. This is a SOP, so $x_1, \dots, x_t$ are parameters.

On the other hand, if $x_1, \dots, x_t$, are parameters, extend to a SOP $x_1, \dots, x_d$. If I is the image of $(x_{t+1}, \dots, x_d)$ in $R' = R/(x_1, \dots, x_t)$, we have R'/I is zero-dimensional so I is $\mathfrak{m}$-primary in R'. Thus, $\dim(R')$ is equal to the height of I, which is then $\leqslant d - t$ by Krull height. That is, $\dim(R') \leqslant d - t$, and using the first statement, we have equality.

(3) This follows from the previous statement and the observation that $\dim(S/(f)) \lneq \dim(S)$ if and only if f is not in any absolutely minimal prime of S. □

Lecture of April 13, 2022

Example 8.16. Note that the first inequality can fail outside of the local case.

(1) Let $R = \dfrac{K[x,y,z]}{(xy, xz, x^2 - x)}$. This ring has dimension two: $A = K[y,z]$ is a Noether normalization, as $x^2 - x = 0$ makes x integral over A, and no nonzero polynomial in y, z withing $K[x,y,z]$ can belong to the ideal $(x) \supseteq (xy, xz, x^2 - x)$. However, $R/(x-1) \cong \dfrac{K[x,y,z]}{(y,z,x-1)} \cong K$ has dimension zero.
(2) Let $R = \mathbb{Z}_{(2)}[x]$. This ring has dimension at least two, but $R/(2x-1) \cong \mathbb{Q}$ has dimension zero.

Example 8.17. The local ring $R = \dfrac{K[x,y,z]_{(x,y,z)}}{(xy, xz)}$ has dimension two. There are two minimal primes (x) and (y,z); this the local ring of the variety given by a line and a plane at the point where they meet. The element x is not a parameter since x is in the absolutely minimal prime (x); x does not decrease the dimension of R. The element $x - y$ is a parameter, as is not in either of the minimal primes. Likewise y is a parameter even though it is in a minimal prime, just not one of maximal dimension.

To complete these to SOPs, $R/(x-y) \cong \dfrac{K[y,z]_{(y,z)}}{(y^2, yz)}$, so $\{x - y, z\}$ is a SOP; $R/(y) \cong \dfrac{K[x,z]_{(x,y,z)}}{(xz)}$, so $\{y, x - z\}$ is a SOP.

We can use this characterization of dimension to prove an inequality on dimensions of fibers. We will say that a ring homomorphism between local rings is a *local homomorphism* if the image of the maximal ideal fo the source is contained in the maximal ideal of the target.

Proposition 8.18. *Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of Noetherian rings. Then*

$$\dim(R) + \dim(S/\mathfrak{m}S) \geqslant \dim(S).$$

Proof. Let $x_1, \ldots, x_d$ be a system of parameters for R and $y_1, \ldots, y_e$ be elements in S whose images form a system of parameters for $S/\mathfrak{m}S$. Then there is some a, b such that $\mathfrak{m}^a \subseteq (x_1, \ldots, x_d)$ and $\mathfrak{n}^b \subseteq (y_1, \ldots, y_e) + \mathfrak{m}S$. Then

$$\mathfrak{n}^{ab} \subseteq ((y_1, \ldots, y_e) + \mathfrak{m}S)^a \subseteq (y_1, \ldots, y_e) + \mathfrak{m}^a S \subseteq (x_1, \ldots, x_d, y_1, \ldots y_e).$$

By Krull height,

$$\dim(S) = \operatorname{height}(\mathfrak{n}) = \operatorname{height}(\mathfrak{n}^{ab}) \leqslant d + e = \dim(R) + \dim(S/\mathfrak{m}S).$$ □

Lecture of April 15, 2022

9. Hilbert functions

9.1. Hilbert functions of graded rings.

Definition 9.1. If K is a field, the *Hilbert function* of an $\mathbb{N}$-graded K-algebra R is the function $H_R : \mathbb{N} \mapsto \mathbb{N} \cup \infty$ with values $H_R(t) := \dim_K(R_t)$. Similarly, if M is a $\mathbb{Z}$-graded R-module, we define the Hilbert function of M in the same way.

We also define the *cumulative Hilbert function* of R as $\widetilde{H}_R(t) := \dim_K(R_{\leqslant t}) = \sum_{i=0}^{t} H_R(t)$, and similarly for a module M.

Example 9.2. Let K be a field, and $R = K[x,y]/(x^2,y^2)$. This ring has a K-vector space basis by monomials that are not multiples of x^2 and y^2, namely $\{1,x,y,xy\}$. We then find $H_R(0) = 1$, $H_R(1) = 2$, $H_R(2) = 1$, and $H_R(t) = 0$ for $t > 2$.

The key example of a Hilbert function is that of a polynomial ring.

Example 9.3. Let K be a field, and $R = K[x_1,\dots,x_n]$ 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

$$R_t = \bigoplus_{a_1+\cdots+a_n=t} K x_1^{a_1}\cdots x_n^{a_n}.$$

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.,

$$H_R(t) = \binom{t+n-1}{n-1} \quad \text{for } t \geqslant 0.$$

We observe the binomial function here can be expressed as a polynomial in t for $t \geqslant 0$; 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 $-1,\dots,-(n-1)$ 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 $t = -(n-1),\dots,-1$.

While the Hilbert function was a polynomial for $n \in \mathbb{N}$ in this example, this is not always the case. First, we need a graded analogue of Noether normalization.

Lemma 9.4. *Let K be an infinite field, and $f \in R = K[x_1,\dots,x_n]$, with $|x_i| = 1$ be a homogeneous polynomial of degree N. There is a degree-preserving K-algebra automorphism of R given by $\phi(x_i) = x_i + a_i x_n$ for $i < n$ and $\phi(x_n) = x_n$ that maps f to a polynomial that viewed as a polynomial in x_n with coefficients in $K[x_1,\dots,x_{n-1}]$, has leading term kx_n^N for some (nonzero) $k \in K$.*

Proof. We just need to show that the x_n^N coefficient is nonzero for some choice of a's. You can check that the coefficient of the x_n^N term is $f(-a_1,\dots,-a_{n-1},1)$. But if this, thought of as a polynomial in the a's, is identically zero, then f must be the zero polynomial. □

Optional Exercise 9.5. Let K be an infinite field, and R be a finitely standard graded K-algebra; recall that this means that R is generated by elements of degree one. Then there are $d = \dim(R)$ algebraically independent elements $z_1,\dots,z_r$ of degree one in R such that $K[z_1,\dots,z_r] \subseteq R$ is module-finite.

We call such a subring a *homogeneous Noether normalization*.

Example 9.6. Let K be a field, and $R = K[x_0,\dots,x_n]$ be a polynomial ring with the standard grading. Let f be an element of degree d. We will compute the Hilbert function of R/fR. Note first that we can apply $- \otimes_K L$ for a larger field L to obtain a ring with the same Hilbert function with an infinite ground field. Then, after applying a degree-preserving coordinate change, we can assume that f is monic in the variable x_0. Then R/fR has $R' = K[x_1,\dots,x_n]$ as a homogeneous Noether normalization, and

$R/fR = R' \cdot 1 + R' \cdot x_0 + \cdots + R' \cdot x_0^{d-1}$ as R'-modules. In fact, this set is a free R'-module basis; any R'-relation on these elements would yield an algebraic relation on $\{x_0, \ldots, x_n\}$ of x_0-degree less than d, which cannot be a multiple of (f). Thus, we have

$$(R'/fR)_t = R'_t \oplus R'_{t-1} \cdot x_0 \oplus \cdots \oplus R'_{t-d+1} \cdot x_0^{d-1}$$

as K-vector spaces for each t. We then have

$$H_{R/fR}(t) = H_{R'}(t) + H_{R'}(t-1) + \cdots + H_{R'}(t-d+1).$$

If $d \leqslant n$, then for all $i = 0, \ldots, d-1$ and all $t \geqslant 0$ we have $t - i > -n$, so by the polynomial ring example, we have $H_{R'}(t-i) = P_n(t-i)$ for each such i and all $t \geqslant 0$, so the Hilbert function agrees with a polynomial for all $t \geqslant 0$.

Now, we suppose that $d > n$, so $d - n - 1 \geqslant 0$. Using that $P_n(t) = H_{R'}(t)$ for $t \geqslant -n$ and $P_n(-n) \neq 0 = H_{R'}(-n)$,

$$\begin{aligned} H_{R/fR}(d-n-1) &= H_{R'}(d-n-1) + H_{R'}(d-n-2) + \cdots + H_{R'}(-n+1) + H_{R'}(-n) \\ &= P_n(d-n-1) + P_n(d-n-2) + \cdots + P_n(-n+1) + 0 \\ &\neq P_n(d-n-1) + P_n(d-n-2) + \cdots + P_n(-n+1) + P_n(-n). \end{aligned}$$

However, for all $t > d - n - 1$, we have that

$$H_{R/fR}(t) = P_n(t) + P_n(t-1) + \cdots + P_n(t-d+1).$$

Thus, if $H_{R/fR}(t)$ agrees with an element of $\mathbb{Q}[t]$ for all $t \in \mathbb{N}$, it must be the polynomial

$$P_n(t) + P_n(t-1) + \cdots + P_n(t-d+1),$$

but since these are not equal for $t = d - n - 1$, $H_{R/fR}(t)$ does not agree with any element of $\mathbb{Q}[t]$ for all $t \in \mathbb{N}$.

We summarize this example.

Proposition 9.7. *Let $R = K[x_0, \ldots, x_n]/(f)$ where f is homogeneous of degree d in the standard grading; note that $n = \dim(R)$. Then,*

1. *R is a free module of rank d over a (standard graded) homogeneous Noether normalization.*
2. *If $d \leqslant n$, then $H_R(t)$ is a polynomial for all $t \in \mathbb{N}$.*
3. *If $d > n$, then $H_R(t)$ is not a polynomial for all $t \in \mathbb{N}$, but is a polynomial for $t \geqslant d - n$.*

Lecture of April 18, 2022

Out next big goal is to prove that the Hilbert function of a graded module is always eventually equal to a polynomial. We need more graded analogues of tools from earlier.

Lemma 9.8. *If R is a Noetherian $\mathbb{N}$-graded ring and M is a nonzero $\mathbb{Z}$-graded module, then M has a homogeneous associated prime.*

Proof. Consider the set of ideals $\{\operatorname{ann}_R(m) \mid m \in M \smallsetminus 0 \text{ homogeneous}\}$. If M is nonzero, this set is nonempty, so it has a maximal element, say I. Note that I (or any other element of the set above) is homogeneous: if $fm = 0$, writing $f = f_{a_1} + \cdots + f_{a_b}$ as a sum of homogeneous pieces, then $0 = fm = f_{a_1}m + \cdots + f_{a_b}m$ is a sum of elements of different degrees, so $f_{a_i}m = 0$ for each i. Then exactly as in the nonhomogeneous case, one can show that I is prime. $\square$

Definition 9.9. Let R be a Noetherian $\mathbb{N}$-graded ring and M be a finitely $\mathbb{Z}$-graded module. A *homogeneous prime filtration* for M is a prime filtration

$$M = M_t \supsetneqq M_{t-1} \supsetneqq M_{t-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

with $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(t_i)$ as graded modules for homogeneous primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$ and integers t_i, where $N(a)$ is the module with $N(a)_b = N_{a+b}$.

Optional Exercise 9.10. Let R be a Noetherian $\mathbb{N}$-graded ring and M be a finitely $\mathbb{Z}$-graded module.

(1) M has a homogeneous prime filtration.
(2) Every associated prime of M is homogeneous.

We will see that the Hilbert function is always eventually equal to a polynomial, as in the last example. To be precise:

Definition 9.11. A function $f : \mathbb{N} \to \mathbb{Q}$ is *eventually equal to a polynomial* $P \in \mathbb{Q}[t]$ if there is some $N \in \mathbb{N}$ such that $f(t) = P(t)$ for all $t \geqslant N$.

Note that a function can be eventually equal to at most one polynomial, since given two such polynomials, their values would agree on an infinite set.

We prepare with a lemma.

Lemma 9.12. *Let R be a graded ring.*

(1) *Let $0 \to L \to M \to N \to 0$ be a degree-preserving short exact sequence of graded R-modules. Then $H_M(t) = H_L(t) + H_N(t)$.*
(2) *Let*
$$M = M_m \supsetneqq M_{m-1} \supsetneqq M_{m-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$
be a homogeneous Noether normalization with $M_i/M_{i-1} \cong (R/\mathfrak{p}_i)(d_i)$ as graded modules for homogeneous primes $\mathfrak{p}_i \in \operatorname{Spec}(R)$ and integers d_i. Then $H_M(t) = \sum_{i=1}^m H_{R/\mathfrak{p}_i}(t + d_i)$.

Proof. (1) In every degree t we get short exact sequences of vector spaces $0 \to L_t \to M_t \to N_t \to 0$, and the claim follows.
(2) This follows from observation that $H_{L(d)}(t) = H_L(t + d)$ plus the the first part by induction. □

And one more fact to prepare.

Lemma 9.13. *Let R be a Noetherian ring and M be a finitely generated R-module. For any prime filtration*

$$M = M_m \supsetneqq M_{m-1} \supsetneqq M_{m-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

of M with $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ (as R-modules, without any respect to grading in the graded case), we have $\dim(M) = \max\{\dim(R/\mathfrak{p}_i) \mid i = 1, \ldots, m\}$.

Proof. We have

$$\begin{aligned}\dim(M) &= \dim(R/\operatorname{ann}_R(M)) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in V(\operatorname{ann}_R(M))\} \\ &= \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Supp}_R(M)\} = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Ass}_R(M)\}.\end{aligned}$$

Since

$$\operatorname{Ass}_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} \subseteq \operatorname{Supp}_R(M),$$

the equality follows. □

Recall that the dimension of a module M is the dimension of $R/\operatorname{ann}_R(M)$.

Theorem 9.14. *Let K be a field, and R be a finitely generated standard graded K-algebra. Let M be a finitely generated graded R-module. Then there is a polynomial $P_M(t) \in \mathbb{Q}[t]$ and some $n \in \mathbb{N}$ such that $H_M(t) = P_M(t)$ for $t \geqslant n$. Moreover, $\deg(P_M) = \dim(M)-1$ and $(\dim(M)-1)!$ times the leading coefficient is a positive integer; if $\dim(M) = 0$, then $P_M = 0$.*

Proof. We show by induction on the dimension of M that this holds for all rings R satisfying the hypotheses. If the dimension of M is zero, then in any prime filtration of M, any factor has dimension zero, so the prime filtration is a composition series, so M has finite length. Thus, it must be finite dimensional as a vector space, so only finitely many graded pieces can be nonzero.

Now, suppose M has dimension n and assume the result for modules of smaller dimension. We first deal with prime cyclic modules. If $M = R/\mathfrak{p}_i$, then take a homogeneous Noether normalization A for this K-algebra M, and consider a homogeneous prime filtration for M as an A-module:

$$M = M_m \supsetneqq M_{m-1} \supsetneqq M_{m-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

with $M_i/M_{i-1} \cong A/\mathfrak{p}_i(d_i)$ for some homogeneous primes $\mathfrak{p}_i \subset A$ and integers d_i. Every factor is either a shift of A, or else has dimension less than $a := \dim(A) = \dim(M)$, since A is a domain; then by the Lemma, at least one factor is a shift of A. Applying the induction hypothesis and the formula $H_M(t) = H_{R/\mathfrak{p}_1}(t+d_1) + \cdots + H_{R/\mathfrak{p}_m}(t+d_m)$ from the Lemma to this context, we find that $H_M(t)$ is a sum of shifts of the polynomial $P_a(t)$ from the example above, plus polynomials of lower degree. Shifting a polynomial does not affect the leading term, so the claim holds.

Now for general M of dimension n, take a homogeneous prime filtration over R,

$$M = M_m \supsetneqq M_{m-1} \supsetneqq M_{m-2} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$

with $M_i/M_{i-1} \cong R/\mathfrak{p}_i(d_i)$ for some homogeneous primes $\mathfrak{p}_i \subset R$ and integers d_i. By the Lemma, $H_M(t) = H_{R/\mathfrak{p}_1}(t+d_1) + \cdots + H_{R/\mathfrak{p}_m}(t+d_m)$. By the Lemma, we have $\dim(R/\mathfrak{p}_i) \leqslant n$ with equality for all i. Then the result follows from the prime cyclic case. This completes the induction. □

Definition 9.15. The *Hilbert polynomial* of a graded module is the polynomial $P_M(t)$ that agrees with $H_M(t)$ for $t \gg 0$. The *multiplicity* of a nonzero M is $(\dim(M)-1)!$ times the leading coefficient of $P_M(t)$, denoted $e(M)$, which is a positive integer.

Proposition 9.16. *Let K be a field, and R be a standard graded finitely generated K-algebra. Let*

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

be a degree-preserving short exact sequence of graded R-modules. Then $P_M(t) = P_L(t) + P_N(t)$. If $\dim(L) = \dim(M) = \dim(N)$, then $e(M) = e(L) + e(N)$.

Proof. Both claims follow from the fact that Hilbert functions are additive on short exact sequences. □

Example 9.17. If R is a polynomial ring, then $e(R) = 1$. If $R = S/fS$ for a polynomial ring S and a homogeneous element f of degree d, then $e(R) = d$.

We want to state analogous results for the cumulative Hilbert function. The point is the following.

Lemma 9.18. *Let $f : \mathbb{N} \to \mathbb{Q}$ be a function, and $F : \mathbb{N} \to \mathbb{Q}$ be the function given by $F(t) = \sum_{i=0}^{t} f(i)$.*

(1) *$f(t)$ is eventually equal to a polynomial if and only if $F(t)$ is eventually equal to a polynomial.*

(2) *If $f(t)$ is eventually equal to $p(t)$ and $F(t)$ is eventually equal to $P(t)$, then* $\deg(P) = \deg(p) + 1$, *and the leading coefficient of P times* $\deg(P)!$ *equals the leading coefficient of p times* $\deg(p)!$.

Proof. First, we note that if we set $c_n(t) = \dfrac{t(t-1)\cdots(t-n+1)}{n!}$ and $c_0(t) = 1$, then $c_n(t)$ is a polynomial of degree n, and $c_n(t) = \binom{t}{n}$ for all "reasonable values" $t \geqslant n$; considering the roots of the polynomials, the equality holds for all $t \geqslant 0$, in fact. We recall binomial identities

$$\binom{t}{n} = \binom{t-1}{n} + \binom{t-1}{n-1} \qquad \text{and} \qquad \sum_{i=0}^{t} \binom{i}{n} = \binom{t+1}{n+1}.$$

The first arises from fixing an element x in a set X of t elements; the subsets Y of size n either contain X or do not; the collection of subsets Y containing x are in bijection with sets $Y \smallsetminus x$ of $X \smallsetminus x$ of size $t-1$, of which there are $\binom{t-1}{n-1}$; those that do not contain x are in bijection with subsets Y of $X \smallsetminus x$ of size t, of which there are $\binom{t}{n-1}$. The second arises by identifying a subset Y of $\{1, \ldots, t+1\}$ of size $n+1$ with the pair $\{\min(Y), Y \smallsetminus \min(Y)\}$; fixing $\min(Y)$, there are $\binom{t - \min(Y)}{n}$ choices for $Y \smallsetminus \min(Y)$.

Thus, the polynomials

$$c_n(t) - c_n(t-1) - c_{n-1}(t-1) \qquad \text{and} \qquad c_{n+1}(t+1) - \sum_{i=0}^{t} c_n(i)$$

have infinitely many zeroes in $\mathbb{Q}$, and hence are each the zero polynomial; thus we have the corresponding identities to above for the polynomials $c_n(t)$. The functions $\{c_0, \ldots, c_j\}$ form a basis for the set of polynomials of degree at most j.

If for $t \geqslant N$, $f(t)$ is equal to a polynomial $p(t)$ of degree n and leading coefficient a, then write

$$p(t) = n!ac_n(t) + b_{n-1}c_{n-1}(t) + \cdots + b_0c_0(t).$$

Then for $t \geqslant N$,

$$\begin{aligned} F(t) = \sum_{i=0}^{t} f(i) &= \sum_{i=0}^{N-1} f(i) + \sum_{i=N}^{t} p(i) \\ &= \sum_{i=0}^{N-1} (f(i) - p(i)) + \sum_{i=0}^{t} p(i) \\ &= n!ac_{n+1}(t) + b_{n-1}c_n(t) + \cdots + b_0c_1(t) + \left(\sum_{i=0}^{N-1} (f(i) - p(i)) \right), \end{aligned}$$

which is a polynomial of degree $n+1$ and leading coefficient $\dfrac{n!a}{(n+1)!}$.

Conversely, if for $t \geqslant N$, $F(t)$ is eventually equal to a polynomial $P(t)$ of degree $n+1$ and leading coefficient a, then write

$$P(t) = (n+1)!ac_{n+1}(t) + b_nc_n(t) + \cdots + b_0c_0(t).$$

Then for $t \geqslant N+1$,

$$\begin{aligned} f(t) &= F(t) - F(t-1) \\ &= ((n+1)!ac_{n+1}(t) + b_nc_n(t) + \cdots + b_0c_0(t)) - ((n+1)!ac_{n+1}(t-1) + b_nc_n(t-1) + \cdots + b_0c_0(t-1)) \\ &= (n+1)!ac_n(t-1) + b_nc_{n-1}(t-1) + \cdots + b_1c_0(t-1) \end{aligned}$$

which is a polynomial of degree n and leading coefficient $\dfrac{(n+1)!a}{n!}$. □