Contents

Chapter 0

Conventions

All rings, unless specified otherwise, are commutative and associative with $1 \neq 0$.

All ideals I are assumed to be strict subsets $I \neq R$. We will call the unit "ideal" an improper ideal.

All modules satisfy the condition $1 \cdot m = m$ for all $m \in M$.

Chapter 1

Finiteness conditions

13 Agosto

1.1 Finitely generated algebras

Let $\varphi : A \to R$ be a ring homomorphism. Another piece of terminology for this situation is to say that R is an *A-algebra*. An A-algebra is a ring R and a homomorphism $\varphi : A \to R$; the same ring R with two different maps $\varphi, \varphi' : A \to R$ yields two different A-algebras.

When R is an A-algebra, we will sometime abuse notation and write $a \in A$ for its image $\varphi(a) \in R$; this is not an abuse if $A \subseteq R$.

A set of elements $\Lambda \subseteq R$ *generates* R as an A-algebra if the following equivalent conditions hold: This can be unpackaged more concretely in a number of equivalent ways:

1. The only subring of R containing A and Λ is R itself.
2. Every element of R admits a polynomial expression in Λ with coefficients in $\varphi(A)$.
3. The homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on $|\Lambda|$ indeterminates, and $\psi(x_i) = \lambda_i$, is surjective.

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 $f_1, \ldots, f_t \in R$ that generates R as an A-algebra. The term *finite-type* is also used to mean this. A better name might be *finitely generatable*, since to say that an algebra is finitely generated does not require knowing any actual finite set of generators.

From the discussion above and the first isomorphism theorem, R is a finitely generated A-algebra if and only if R is a quotient of some polynomial ring $A[x_1, \ldots, x_d]$ over A in finitely many variables. If R is generated over A by $f_1, \ldots, f_d$, we will use the notation $A[f_1, \ldots, f_d]$ to denote R. Of course, for this notation to properly specify a ring, we need to understand how these generators behave under the operations. This is no problem if A and $\underline{f}$ are understood to be contained in some larger ring.

A quick observation: any surjective φ is algebra-finite: the target is generated by 1. Since any homomorphism $\varphi : A \to R$ can be factored as the surjection $A \to A/\ker(\varphi)$ followed by the inclusion $A/\ker(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms.

Remark 1.1. Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $A \subseteq B$ algebra-finite and $B \subseteq C$ algebra-finite $\implies A \subseteq C$ algebra-finite, and
- $A \subseteq C$ algebra-finite $\implies B \subseteq C$ algebra-finite.

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

Example 1.2. Let $A = K$ be a field, and $B = K[x, xy, xy^2, xy^3, \cdots] \subseteq C = K[x, y]$, where x and y are indeterminates. Any finitely generated subalgebra of B is contained in $K[x, xy, \ldots, xy^m]$ for some m, since we can write the elements in any finite generating set as polynomial expressions in the finitely many specified generators of B. But, every element of $K[x, xy, \ldots, xy^m]$ is a K-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated A-algebra.

Let R be an A-algebra and $\Lambda \subseteq R$. The ideal of *relations* on the elements Λ over A is the kernel of the map $\psi : A[X] \to R$, $\psi(x_i) = \lambda_i$: this is the polynomial functions with A-coefficients that the elements of Λ satisfy. Given an A-algebra R with generators Λ and ideal relations I, we have $R \cong A[X]/I$ by the first isomorphism theorem. Thus, if we understand A and generators and relations for R over A, we can get a pretty concrete understanding of R. If a sequence of elements has no nonzero relations, we say they are *algebraically independent* over A.

There are many basic questions about 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? It isn't 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 Integral extensions

We will also find it quite useful to consider a stronger finiteness property for maps. Recall that if $\varphi : A \to R$ is a ring homomorphism, then R acquires an A-module structure via φ by $a \cdot r = \varphi(a)r$; this is a particular case of *restriction of scalars*. We may write ${}_\varphi R$ for this A-module if we think we will have trouble remembering the map. Of course, if φ is injective and we identify it with the inclusion $A \subseteq R$, then this A-action is just $a \cdot r = ar$.

Recall that an A-module M is generated by a set of elements $\Gamma \subseteq M$ if the only submodule of M that contains Γ is M itself. This also has some equivalent realizations:

1. Γ generates M as an A-module.
2. Every element of M admits a linear combination expression in Γ with coefficients in A.
3. The homomorphism $\theta : A^{\oplus Y} \to M$, where $A^{\oplus Y}$ is a free A-module on $|\Gamma|$ basis elements, and $\theta(y_i) = \gamma_i$, is surjective.

We recall that a *basis* for an R-module is a generating set Γ such that $\sum_i a_i\gamma_i = 0$ implies all $a_i = 0$, for $a_i \in R$, $\gamma_i \in \Gamma$; a *free module* is a module that admits a basis. Every ring that is not a field admits a non-free module, namely the cyclic module R/I for an ideal $I \subseteq R$.

We use the notation $M = \sum_{\gamma \in \Gamma} A\gamma$ to indicate that M is generated by Γ as a module. We say that $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module. This is also called

simply *finite* in the literature; we will see why in a few weeks, but we'll stick with the unambiguous "module-finite."

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

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

Example 1.3.

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 $\{1, x, x^2, x^3, \dots\}$.

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 and 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 $M \subseteq 1/x^N \cdot K[x] \neq K[x, 1/x]$.

Lemma 1.4. *If $R \subseteq S$ is module-finite, and N is a finitely generated S-module, then N is a finitely generated R-module by restriction of scalars. In particular, the composition of two module-finite ring maps is module-finite.*

Proof. Let $S = \sum_{i=1}^{r} Ra_i$ and $N = \sum_{j=1}^{s} Sb_j$. Then, $N = \sum_{i=1}^{r} \sum_{j=1}^{s} Ra_ib_j$: given $n = \sum_{j=1}^{s} s_j b_j$, rewrite each $s_j = \sum_{i=1}^{r} r_{ij} a_i$ and substitute to get $t = \sum_{i=1}^{r} \sum_{j=1}^{s} r_{ij} a_i b_j$ as an R-linear combination of the $a_i b_j$. □

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

Definition 1.5 (Integral element/extension)**.** *Let $\varphi : A \to R$ be a ring homomorphism, 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.*

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

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

Evidently, integral implies algebraically dependent, and the condition that there exists an equation of algebraic dependence that is *monic* is stronger in the setting of rings.

Proposition 1.6. *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, given a polynomial in $p(r)$ of degree $\geq n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in r.

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

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

15 Agosto

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

Lemma 1.7 (Determinant 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 fact. We deduce the case of a general commutative ring from the field case.

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

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

Theorem 1.8 (Module finite implies integral)**.** *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

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

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

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

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

Corollary 1.9 (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 rest 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 1.6. □

Corollary 1.10. *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,

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

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

Definition 1.11. *If $A \subseteq R$, the* integral closure of A in R *is the set of elements of R that are integral over A.*

Example 1.12.

1. Let $R = \mathbb{C}[x, y] \subseteq S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$. 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.
2. Let $R = \mathbb{C}[u, v] \subseteq S = \mathbb{C}[u, v, w]/(u^2 + vw)$. (Note that this S is isomorphic to the previous S by the map $u \mapsto x, v \mapsto y + iz, w \mapsto y - iz$, and this R corresponds to the polynomial subring $\mathbb{C}[x, y + iz]$.) We claim that S is *not* integral and hence *not* module-finite over R. Indeed, the minimal polynomial of w over the fraction field of R is $f(t) = vt + u^2$. Any equation that w satisfies is a $\mathbb{C}(u, v)[t]$-multiple of this: write $g(t) = f(t)h(t)$ with $g(t) \in \mathbb{C}(u, v)[t]$ monic. By Gauss' lemma, there is some $a \in \mathbb{C}(u, v)$ such that $a^{-1}f(t), ah(t) \in \mathbb{C}[u, v][t]$. Since the leading coefficient of h is v^-1, the numerator of a must be a multiple of v when written in lowest terms. But this contradicts that $a^{-1}f(t) \in \mathbb{C}[u, v][t]$.
3. Not all integral extensions are module-finite. Let $K = \overline{K}$, and consider the ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots] \subseteq \overline{K(x)}$. Clearly R is generated by integral elements over $K[x]$, but is not algebra-finite over $K[x]$. (Prove it!)

Remark 1.13. Let $A \subseteq B \subseteq C$ be rings. As with algebra-finiteness, it follows from the definitions that

- $A \subseteq B$ module-finite and $B \subseteq C$ module-finite $\implies A \subseteq C$ module-finite, and
- $A \subseteq C$ module-finite $\implies B \subseteq C$ module-finite,

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

1.3 Noetherian rings and modules

We now discuss an absolute, rather than relative, finiteness condition for a ring R.

Definition 1.14 (Noetherian ring)**.** *A ring R is* Noetherian *if every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ eventually stabilizes: there is some N for which $I_n = I_{n+1}$ for all $n > N$.*

This condition also admits some equivalences.

Proposition 1.15 (Equivalences for Noetherian ring)**.** *The following are equivalent for a ring R.*

1. *R is a Noetherian ring.*
2. *Every nonempty family of ideals has a maximal element (under containment).*
3. *Every ascending chain of finitely generated ideals of R eventually stabilizes.*
4. *Given any generating set S for an ideal I, the ideal I is generated by a finite subset of S.*
5. *Every ideal of R is finitely generated.*

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

(2)⇒(1): Clear.

(1)⇒(3): Clear.

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

(4)⇒(5): Clear.

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

Example 1.16.

1. If K is a field, the only ideals in K are (0) and $(1) = K$, so K is Noetherian.
2. If R is a PID, then R is Noetherian. Every ideal is finitely generated!
3. As a special case of the previous, 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 $z^n g(z)$ with $g(z) \neq 0$, 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: 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. Another ring that is *not* Noetherian is the ring $R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \ldots] \subseteq \overline{K(x)}$ from earlier. A nice ascending chain of ideals is
$$(x) \subseteq (x^{1/2}) \subseteq (x^{1/3}) \subseteq (x^{1/4}) \subseteq \cdots.$$
6. A variation on the last example: the ring of *nonnegatively valued Puiseux series*: $R = \bigcup_{n\in\mathbb{N}} \mathbb{C}[\![z^{1/n}]\!] \subseteq \overline{\mathbb{C}((z))}$.[1]

[1] In fact, the algebraic closure of the field of Laurent series $\mathbb{C}((z))$ is $\bigcup_{n\in\mathbb{N}} \mathbb{C}((z^{1/n})) = R[1/t]$.

7. 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!

Definition 1.17 (Noetherian module)**.** *An R-module M is* Noetherian *if every ascending chain of submodules of M eventually stabilizes.*

There are analogous criteria for modules to (1)–(5) above namely:

Proposition 1.18 (Equivalences for Noetherian module)**.** *The following are equivalent for a module M:*

1. *M is a Noetherian module.*
2. *Every nonempty family of submodules has a maximal element.*
3. *Every ascending chain of finitely generated submodules of M eventually stabilizes.*
4. *Given any generating set S for a submodule N, the submodule N is generated by a finite subset of S.*
5. *Every submodule of M is finitely generated.*

In particular, a Noetherian module must be finitely generated.

We observe that if R is Noetherian, and I is an ideal of R, then R/I is Noetherian as well, since there is an order-preserving bijection

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

Lemma 1.19. *Let M be a module, and M', M'', N be submodules of M.*

1. *Then $M' = M''$ if and only if $M' \cap N = M'' \cap N$ and $M'/(M' \cap N) = M''/(M'' \cap N)$.*
2. *M is Noetherian if and only if N and M/N Noetherian.*

Proof. 1. ($\Rightarrow$) is clear. Suppose that $M' \subsetneq M''$ and $M' \cap N = M'' \cap N$. Then, there is some $m \in M'' \smallsetminus M'$. We claim that the class of m in $M''/(M'' \cap N)$ is not equal to the class of m' in $M''/(M'' \cap N)$ for any $m' \in M'$. Indeed, if it were, then $m - m' \in M'' \cap N = M' \cap N$, so that $m \in M' + M' \cap N = M'$, a contradiction.

2. A chain of submodules of N is a chain of submodules of M, and a (proper) chain of submodules of M/N lifts to a (proper) chain of submodules of M, so M Noetherian implies N and M/N are. Conversely, if N and M/N are Noetherian, then for any chain

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

of submodules of M, the chains

$$(M_0 \cap N) \subseteq (M_1 \cap N) \subseteq (M_2 \cap N) \subseteq \cdots$$

in N and

$$\frac{M_0}{M_0 \cap N} \subseteq \frac{M_1}{M_1 \cap N} \subseteq \frac{M_2}{M_2 \cap N} \subseteq \cdots$$

in M/N stabilize eventually. If both chains are stable past index n, then the chain in M is stable past index n by part 1. □

Proposition 1.20. *Let R be a Noetherian ring. Then M is a Noetherian module if and only if M is finitely generated.*

Consequently, if R is Noetherian, then any submodule of a finitely generated R-module is also finitely generated.

Proof. If M is Noetherian, it (and all of its submodules) is finitely generated by the equivalences above.

Now let R be Noetherian and M be f.g.. First, we show that the free module $R^{\oplus n} = \bigoplus_{i=1}^{n} Re_i$ is Noetherian for all $n \in \mathbb{N}$ by induction on n. For the base case, we note that R is a Noetherian ring iff the free cyclic module $R^{\oplus 1}$ is a Noetherian module, since ideals of R correspond to submodules of $R^{\oplus 1}$. The inductive step follows since we have an isomorphism $(\bigoplus_{i=1}^{n} Re_i)/Re_n \cong \bigoplus_{i=1}^{n-1} Re_i$. Now, a finitely generated module M is quotient of a finitely generated free module, so is Noetherian by the previous lemma. □

20 Agosto

It is now clear that a module-finite extension R of a Noetherian ring A is Noetherian: R is a Noetherian A-module, and any ideal of R is an A-submodule of R, so an ascending chain necessarily stabilizes.

Here is a stronger statement:

Theorem 1.21 (Hilbert Basis Theorem)**.** *Let A be a Noetherian ring. Then $A[x_1, \ldots, x_d]$ and $A[\![x_1, \ldots, x_d]\!]$ are Noetherian.*

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

By induction on d, we reduce to the case $d = 1$. Let $I \subseteq A[x]$, and let

$$J = \{a \in A \mid \exists\, ax^n + \text{lower order terms (wrt } x) \in I\}.$$

This is easily seen to be an ideal of A, which is finitely generated by hypothesis; let $J = (a_1, \ldots, a_t)$. Pick $f_1, \ldots, f_t \in A[x]$ such that the leading coefficient of f_i is a_i, and set $i' = (f_1, \ldots, f_t)$. Let $N = \max_i \deg f_i$.

Given $f \in I$ of degree greater than N, we can cancel off the leading term of f by subtracting a suitable multiple of some f_i, so any $f \in I$ can be written as $g + h$ with $g \in I \cap \sum_{i=0}^{N} Ax^i$ and $h \in I'$. Since $I \cap \sum_{i=0}^{N} Ax^i$ is a submodule of a finitely generated free A-module, it is also finitely generated as an A-module. Given such a generating set, we can clearly write any such f as an $A[x]$-linear combination of these generators and the f_i's.

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

Corollary 1.22. *If A is a Noetherian ring, then any finitely generated A-algebra is Noetherian. In particular, any finitely generated algebra over a field is Noetherian.*

The converse to this statement is false: there are lots of Noetherian rings that are not f.g. algebras over a field. For example, $\mathbb{C}\{z\}$ is not algebra-finite over $\mathbb{C}$. You will show (modulo some steps) that rings of power series and rings of complex functions analytic near a point are both Noetherian. We will also see huge classes of easy examples once we switch to localization. However, we'll see a converse in a very special case soon.

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

Theorem 1.23 (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 $C = A[f_1, \ldots, f_r]$ and $C = \sum_{i=1}^{s} Bg_i$. Then,

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

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

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

1.4 Application: Invariant rings

Question 1.24. Given a (finite) set of symmetries, one can consider the collection of polynomial functions that are fixed by all of them. Is there a finite set of fixed polynomials such that any fixed polynomial can be expressed in terms of them?

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 $R = K[x_1, \ldots, x_d]$ is a polynomial ring over a field. We are interested in the set of elements that are *invariant* under the action

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

If $r, s \in R^G$, then

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

since each g is a homomorphism. Thus, R^G is a subring of R.

We note that if $G = \langle g_1, \ldots, g_t \rangle$, then $r \in R^G$ if and only if $g_i(r) = r$ for $i = 1, \ldots, t$.

We will especially be generated by *linear actions*: G acts linearly on a polynomial ring $R = K[x_1, \ldots, x_n]$ if every element of g satisfies $g \cdot k = k$ for all $k \in K$ and $g \cdot x_i$ is a linear form in R for all i.

Example 1.25 (Standard representation of the symmetric group)**.** Let $\mathcal{S}_d$ be the symmetric group on d letters acting on $R = K[x_1, \ldots, x_d]$ via $\sigma(x_i) = x_{\sigma_i}$.

For example, if $d = 3$, 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.

It is a theorem that you may have seen this in an earlier algebra class that every element of R^G can be written as polynomial expression in the elementary symmetric polynomials $e_i = \sum_{I \subseteq [d],\, |I| = i} \left(\prod_{j \in I} x_j\right)$. E.g, f above is $e_1^2 - 2e_2$.

Example 1.26 (Roots of unity)**.** Let $G = \{e, g\}$ act on $R = K[x_1, \ldots, x_d]$ by negating the variables: $g \cdot x_i = -x_i$ for all i, so $g \cdot f(\underline{x}) = f(-\underline{x})$. Suppose that the characteristic of K is not 2, so $-1 \neq 1$. Given a general f, we can write it as a sum of its *homogeneous* pieces: that is,

$$f = f_r + f_{r-1} + \cdots + f_1 + f_0,$$

where each f_i is a sum of monomials of degree i. We have $g(f_i) = (-1)^i f_i$, so

$$g(f) = (-1)^r f_r + (-1)^{r-1} f_{r-1} + \cdots - f_1 + f_0,$$

which differs from f unless every homogeneous piece of f has even degree. That is,

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

This computation readily generalizes to the case of a field K that contains t-th roots of unity, and a cyclic group $G = \langle g \rangle$ of order t acting on R by the rule $g(x_i) = \zeta_t \cdot x_i$ for all i. In this case, we have

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

This ring is called the *t-th Veronese ring*. As an algebra, this ring is generated by the monomials of degree t.

Example 1.27. Some of the most interesting examples come from infinite groups G. Let $X = X_{2\times 3}$, be a matrix of indeterminates, and $\mathbb{C}[X]$ be the polynomial ring on those indeterminates. The group $\mathrm{SL}_2(\mathbb{C})$ acts on the matrix X by left multiplication. Write $X_{\hat{i}}$ for the matrix X with column i removed. If $g \in \mathrm{SL}_2(\mathbb{C})$, then $gX_{\hat{i}} = (gX)_{\hat{i}}$, since left multiplication by g can be computed column-by-column. Thus,

$$\det((gX)_{\hat{i}}) = \det(gX_{\hat{i}}) = \det(g)\det(X_{\hat{i}}) = \det(X_{\hat{i}}).$$

We find that the 2×2 minors of X $(x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{23} - x_{13}x_{21}, x_{12}x_{23} - x_{13}x_{22})$ must be invariant functions. This readily generalizes to $m \times n$ matrices with $m \leq n$ and maximal minors. It is harder to show that these maximal minors generate all of the invariants.

21 Agosto

We now want to move towards answering our question. We will use our various notions of finiteness.

Proposition 1.28. *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. 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.

Now, for $r \in R$, consider the polynomial $F_r(t) = \prod_{g\in G}(t - g(r)) \in R[t]$. Clearly $g(F_r(t)) = F_r(t)$, where G fixes t. Thus, $F_r(t) \in R^G[t]$. The leading term (with respect to t) is $t^{|G|}$, so $F_r(t)$ is monic. Thus, r is integral over R^G. Therefore, R is integral over R^G. □

Theorem 1.29 (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-lienarly 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! □

1.5 Graded rings

A useful bit of extra structure that one commonly encounters, and that we have already used, even, is that of a grading on a ring.

Definition 1.30. *Let R be a ring, and T be a monoid. The ring R is* T-graded *if there exists a direct sum decomposition of R as an abelian group indexed by T: $R = \bigoplus_{a\in M} R_a$ such that, for any $a, b \in T$, and any $r \in R_a, s \in R_b$, one has $rs \in R_{a+b}$.*

An element that lies in one of the summands R_a is said to be homogeneous *of* degree a*; we often use $|r|$ to denote the degree of a homogeneous element r.*

Definition 1.31. *Let R and S be T-graded rings (same grading monoid). A ring homomorphism $\varphi : R \to S$ is* degree-preserving *if $\varphi(R_a) \subseteq S_a$ for all $a \in T$.*

By definition, an element in a graded ring is, in a unique way, a sum of homogeneous elements, which we call its homogeneous components or graded components.

Example 1.32.

1. If K is a field, and $R = K[x_1, \dots, x_n]$ is a polynomial ring, then there is an $\mathbb{N}$-grading on R where R_d is the K-vector space with basis given by monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\sum_i \alpha_i = d$. Of course, this is the notion of degree familiar from grade school. This is called the *standard grading*.

2. With K and R as above, for any $(\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, one can give a different $\mathbb{N}$-grading on R by letting x_i have degree β_i for some integers β_i; we call this a grading with *weights* $(\beta_1, \dots, \beta_n)$.

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

3. Again with K and R as above, R admits an $\mathbb{N}^n$-grading, with $R_{(d_1,\dots,d_n)} = K \cdot x_1^{d_1} \cdots x_n^{d_n}$. This is called the *fine grading*.

4. Let $\Gamma \subseteq \mathbb{N}^n$ be a subsemigroup. Then $\bigoplus_{\gamma\in\Gamma} K\underline{x}^\gamma \subseteq K[\underline{x}]$ is an $\mathbb{N}^n$-graded subring. Conversely, every $\mathbb{N}^n$-graded subring of $K[x_1, \dots, x_n]$ is of this form. (Check it!)

5. 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. (I.e., R^G is graded with respect to the same grading monoid.) In particular, if G acts K-linearly on a polynomial ring over K, the invariant ring is $\mathbb{N}$-graded.

Definition 1.33. *An ideal I in a graded ring R is called* homogeneous *if it is generated by homogeneous elements.*

We observe that an ideal is homogeneous if and only if, for any $f \in R$, one has $f \in I$ if and only if every homogeneous component of f lies in I. To see "if," take a generating set $\{f_\lambda\}_\Lambda$ for I; all of its homogeneous components of each f_λ lie in I, and each f_λ lies in the ideal generated by these components. Thus the set of components generates I. The other direction is also easy.

We now observe the following:

Lemma 1.34. *Let R be an T-graded ring, and I be a homogeneous ideal. Then R/I is also T-graded.*

Example 1.35.

1. The ring $R = K[w, x, y, z]/(w^2x + wyz + z^3, x^2 + 3xy + 5xz + 7yz + 11z^2)$ admits an $\mathbb{N}$-grading with $|w| = |x| = |y| = |z| = 1$.

2. 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 1.36. *Let R be a T-graded ring, and M a module. The module R is* T-graded *if there exists a direct sum decomposition of M as an abelian group indexed by T: $M = \bigoplus_{a \in T} M_a$ such that, for any $a, b \in T$, and any $r \in R_a, m \in R_b$, one has $rm \in M_{a+b}$.*

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 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 1.37. *Let R be an $\mathbb{N}$-graded ring, and $f_1, \ldots, f_n$ be homogeneous elements 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.*

Consequently, R is Noetherian if and only if R_0 is Noetherian and R is algebra-finite over R_0.

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

To show that $R_+ = (f_1, \ldots, f_n)$ implies $R = R_0[f_1, \ldots, f_n]$, 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, $r \in R_+$ so we can write $r = a_1 f_1 + \cdots + a_n f_n$; moreover, we can do so with each a_i 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 consequently statement, if R_0 is Noetherian and R algebra-finite over R_0, then R is Noetherian by Hilbert Basis. If R is Noetherian, R_0 is Noetherian, since it is isomorphic to R/R_+, and 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. □

1.6 Application: Invariant rings, reprise

With the basics of graded rings in hand, we can 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. We need another notion that is very useful in commutative algebra.

Definition 1.38. *Let R be an A-algebra, where $\phi : A \to R$ is the map from A to R. We say that A is a* direct summand *of R if there is an A-module homomorphism $\pi : R \to A$ such that $\pi \circ \phi$ is the identity on A.*

First, observe that the condition implies that ϕ must be injective, so we can assume that $A \subseteq R$ (perhaps after renaming elements). Then the condition on π is that $\pi(ar) = a\pi(r)$ for all $a \in A$ and $r \in R$ and that $\pi|_A$ is the identity. We call the map π the *splitting* of the inclusion. Note that if $\pi : R \to A$ is A-linear, if $\pi(1) = 1$, then π is a splitting, since $\pi(a) = \pi(a \cdot 1) = a\pi(1) = a$ for all $a \in A$.

Lemma 1.39. *Let A be a direct summand of R. Then, for any ideal $I \subseteq A$, we have $IR \cap A = I$.*

Proof. Let π be the splitting of the inclusion. If $a \in IR \cap A$, we have $a = \sum_{i=1}^{t} r_i f_i$, for $f_i \in I$. Applying π, we have

$$a = \pi(a) = \pi(\sum_{i=1}^{t} r_i f_i) = \sum_{i=1}^{t} \pi(r_i f_i) = \sum_{i=1}^{t} \pi(r_i) f_i \in I.$$

□

Proposition 1.40. *Let A be a direct summand of R. If R is Noetherian, then so is A.*

Proof. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals in A. The chain $I_1R \subseteq I_2R \subseteq I_3R \subseteq \cdots$ stabilizes, so $\exists J, N$ such that $I_nR = J$ for $n \geq N$. Contracting to A, we get that $I_n = I_nR \cap A = J \cap A$ for $n \geq N$, so the chain stabilizes. □

Proposition 1.41. *Let K be a field, and R be a polynomial ring over K. Let G be a finite group acting K-linearly on R. Assume that $|G|$ does not divide the characteristic of K; this condition is trivially satisfied if K has characteristic zero. 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 maps lies in R^G, since acting by g permutes the elements in the sum. Now, we claim that this is a splitting of the inclusion: 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 1.42 (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 K-linearly 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 linearly, 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 the previous proposition. By our characterization of Noetherian graded rings, R^G is finitely generated over $R_0 = K$. □

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

Chapter 2

Nullstellensatz and Spectrum

27 Agosto

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

Question 2.1. To what extent is a system of polynomial equations determined by its solution set?

Example 2.2. Let's consider one polynomial equation in one variable. Over $\mathbb{R}, \mathbb{Q}$, or other fields that aren't algebraically closed, there are many polynomials with an empty solution set. On the other hand, over $\mathbb{C}$, or any algebraically closed field, if $f(z) = 0$ has solutions $z_1, \dots, z_d$, we know that $f(z) = \alpha(z - z_1)^{a_1} \cdots (z - z_d)^{a_d}$, so that f is determined up to scalar multiple and repeated factors. Given any system of polynomial equations $f_1 = \cdots = f_t = 0$, we know that $z = a$ is a solution if and only if it is a solution of $f = 0$, where f is the GCD of $f_1, \dots, f_t$.

Now, let A be any ring. Let $\underline{x} = \{x_\gamma \mid \gamma \in \Gamma\}$ be a set of variables, and $F = \{f_\lambda \mid \lambda \in \Lambda\} \subseteq A[\underline{x}]$ be a set of polynomials. If R is any A-algebra, we can evaluate any polynomial by plugging in elements of R: given $\underline{r} = \{r_\gamma \mid \gamma \in \Gamma\}$, we can evaluate $f(\underline{r})$ in R, and determine whether $f(\underline{r}) = 0$. In this situation, we define the *solution set* to be

$$Z_R(F) := \{\underline{r} \in R^{\oplus \Gamma} \mid f(\underline{r}) = 0 \text{ for all } f \in F\}.$$

In particular, if we are considering a system of polynomial equations in finitely many variables $x_1, \dots, x_n$, then $Z_R(F) \subseteq R^{\oplus n}$. Observe that if $F \subseteq F'$, then $Z_R(F') \supseteq Z_R(F)$. Also, if $\underline{r} \in Z_R(f_1, f_2)$, and $g \in A[\underline{x}]$, then

$$(f_1 + f_2)(\underline{r}) = f_1(\underline{r}) + f_2(\underline{r}) = 0 \qquad \text{and} \qquad (f_1 g)(\underline{r}) = f_1(\underline{r}) g(\underline{r}) = 0,$$

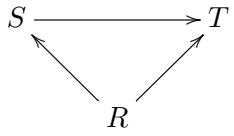
so $Z_R(F) \subseteq Z_R(\,(F)\,)$, and in tandem with the above, equality holds: $Z_R(F) = Z_R(\,(F)\,)$. In particular, by the Hilbert basis theorem, any system of polynomial equations over a field is equivalent to a system of finitely many polynomial equations!

From now on, we will talk about the solution set of an ideal, rather than of an arbitrary set. Observe that if $I = R$ is an *improper ideal*, then $Z_R(I) = \varnothing$, since $1 \neq 0$.

Example 2.3. Let $R = K\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$, and $I = (\Delta_1, \Delta_2, \Delta_3)$, the 2×2-minors of the matrix. Thinking of these generators as equations, a solution is just a matrix of rank at most one, so $Z_K(I)$ is the set of rank at most one matrices. Let $J = (x_1, x_2, x_3)$, and observe that $I \subseteq J$. We then have that $Z_K(J) \subseteq Z_K(I)$: this just translates to the fact that a 2×3 matrix with a zero row has rank at most 1.

2.1 Solutions, algebra homomorphisms, and maximal ideals

We now wish to consider solutions of polynomial equations in great generality. A *homomorphism of R-algebras* from S to T is a ring homomorphism such that



commutes.

Let R be a ring, and S an R-algebra. Let $I \subseteq R[\underline{x}]$ be an ideal. Consider the R-algebra $R[\underline{x}]/I$. If $\underline{a} \in Z_S(I)$ is a solution, so that all $f(\underline{a}) = 0$ for all $f \in I$, then the R-algebra homomorphism from $R[\underline{x}] \to S$ given by $x_i \mapsto a_i$ descends to an R-algebra map $R[\underline{x}]/I \to S$. Conversely, any R-algebra map from $R[\underline{x}]/I$ to S is determined by the images of $\underline{a}$, which must satisfy all of the equations $f_\lambda(\underline{x}) = 0$. We summarize:

Proposition 2.4. *Let R be a ring, and S an R-algebra. Let $I \subseteq R[\underline{x}]$ be an ideal. There is a bijection*

$$\begin{array}{lcl} Z_S(I) & \leftrightarrow & \mathrm{Hom}_{R-\mathrm{alg}}\left(R[\underline{x}]/I, S\right) \\ (a_1, \ldots, a_d) & \mapsto & \varphi|_R = \mathrm{id}, \varphi(x_i) = a_i. \end{array}$$

Now, we focus on polynomial equations over fields.

Proposition 2.5. *Let K be a field, and $R = K[x_1, \ldots, x_d]$ be a polynomial ring. There is a bijection*

$$\begin{array}{lcl} K^d & \leftrightarrow & \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R \textit{ such that } R/\mathfrak{m} \cong K\} \\ (a_1, \ldots, a_d) & \mapsto & (x_1 - a_1, \ldots, x_d - a_d). \end{array}$$

Proof. We observe first that each ideal $(x_1 - a_1, \ldots, x_d - a_d)$ is a maximal ideal with residue field K, and that these ideals are distinct: if $x_i - a_i, x_i - a_i'$ are in the same ideal for $a_i \neq a_i'$, then the unit $a_i - a_i'$ is in the ideal, so it is not proper. To see that the map is surjective, let $\pi : R \twoheadrightarrow K$ be a surjective map. We have $\pi(x_i) \in K$ so $(x_1 - \pi(x_1), \ldots, x_d - \pi(x_d)) \subseteq \mathfrak{m}$. The quotient by this ideal is already K, so $(x_1 - \pi(x_1), \ldots, x_d - \pi(x_d)) = \mathfrak{m}$. □

Theorem 2.6. *Let K be a field, and $R = K[x_1, \ldots, x_d]/I$ be a finitely generated K-algebra. There are bijections*

$$\begin{array}{lcllcl} Z_K(I) & \leftrightarrow & \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R \textit{ s.t. } R/\mathfrak{m} \cong K\} & \leftrightarrow & \mathrm{Hom}_{K-\mathrm{alg}}(R, K) \\ (a_1, \ldots, a_d) \in Z(I) \subseteq K^d & \mapsto & (x_1 - a_1, \ldots, x_d - a_d) & & \\ & & \mathfrak{m} & \mapsto & R \twoheadrightarrow R/\mathfrak{m} \cong K \end{array}$$

Proof. In light of the previous proposition, we need to show that $\underline{a} \in Z_K(I) \Leftrightarrow \mathfrak{m}_{\underline{a}}$ descends to a maximal ideal of R. This boils down to showing that $\underline{a} \in Z_K(I)$ if and only if $I \subseteq \mathfrak{m}_{\underline{a}}$. This follows from the fact that $\underline{a} \in Z_K(I) \Leftrightarrow I \subseteq \ker(\text{evaluation at } \underline{a}) = \mathfrak{m}_{\underline{a}}$. The second map is clearly bijective. □

2.2 A quick word about transcendence bases

We will need the notion of transcendence basis for a field extension shortly, and also later when we return to dimension theory.

Definition 2.7. *Let $K \subseteq L$ be an extension of fields. A* transcendence basis *for L over K is a maximal algebraically independent subset of L.*

Observe that if $\{x_\lambda\}_{\lambda\in\Lambda}$ is a transcendence basis for L over K, then we have 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; 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.

Here is the fact we will use momentarily.

Lemma 2.8. *If $A = \{a_\lambda\}_{\lambda\in\Lambda}$ is a field generating set for L over K, then A contains a transcendence basis for L over K.*

Consequently, any field extension admits a transcendence basis, and a finitely generated field extension admits a finite transcendence basis.

Proof. Observe first that if we have a nested union of algebraically independent sets, the union is algebraically independent; 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. By Zorn's Lemma, we can then pick a maximal algebraically independent (over K) subset A' of A. Any element of $A \smallsetminus A'$ must be algebraic over $K(A')$, and so $L = K(A')(A \smallsetminus A')$ is algebraic over $K(A')$. By the observation above, A' is a transcendence basis. □

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

Theorem 2.9. *Let $K \subseteq L$ be an extension of fields. If X and Y are two transcendence bases for L over K, then $|X| = |Y|$.*

This justifies the following definition.

Definition 2.10. *The* transcendence degree *of a field extension L over K is the common size of any transcendence basis for the extension.*

Observe that the transcendence degree is a lower bound for the size of any field generating set.

29 Agosto

2.3 Maximal ideals of finitely generated algebras

Lemma 2.11 (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.*

Proof. Let $L = K[h_1, \ldots, h_d]$. Since $L = K(h_1, \ldots, h_d)$, we can choose a transcendence basis for L/K from among the h's, and after reordering, we may assume that $h_1, \ldots, h_c = x_1, \ldots, x_c$ form a transcendence basis, and $h_{c+1}, \ldots, h_d$ are algebraic over $K' = K(x_1, \ldots, x_c)$. 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 $K[x_1, \ldots, x_c]$ such that $K' = K[\frac{f_1}{g_1}, \ldots, \frac{f_c}{g_c}]$. This implies that any element of K' can be written as a fraction with denominator $(g_1 \cdots g_c)^n$ for some n. But, the element $\frac{1}{g_1 \cdots g_c + 1} \in K'$ cannot be written this way; if so, we would have

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

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

Corollary 2.12. *Let K be a field, and R be a finitely generated K-algebra. For any maximal ideal $\mathfrak{m}$ of R, $R/\mathfrak{m}$ is a finite extension of K.*

In particular, if K is algebraically closed, $R/\mathfrak{m} \cong K$.

Along similar lines, we have the following:

Exercise 2.13. If R is a finitely generated $\mathbb{Z}$-algebra, and $K = R/\mathfrak{m}$ is a residue field of R, then K is finite.

Corollary 2.14 (Maximal ideals of f.g. $K = \overline{K}$-algebras)**.** *Let K be an algebraically closed field, and $S = K[x_1, \ldots, x_d]$ be a polynomial ring. There is a bijection*

$$K^d \leftrightarrow \{\textit{maximal ideals } \mathfrak{m} \textit{ of } S\}$$

given by $(a_1, \ldots, a_d) \mapsto (x_1 - a_1, \ldots, x_d - a_d)$. If R is a finitely generated K-algebra, we can write $R = S/I$ for a polynomial ring S, and there is an induced bijection

$$Z_K(I) \subseteq K^d \leftrightarrow \{\textit{maximal ideals } \mathfrak{m} \textit{ of } R\}.$$

Theorem 2.15 (Nullstellensatz)**.** *Let K be an algebraically closed field, and $R = K[x_1, \ldots, x_d]$ be a polynomial ring. If $I \subset R$ is an ideal (proper ideal!), then $Z_K(I) \neq \varnothing$.*

Proof. Let $I \subseteq R$ be a proper ideal. Then, there is some maximal ideal $I \subseteq \mathfrak{m}$, and $Z(\mathfrak{m}) \subseteq Z(I)$. We can write $\mathfrak{m} = (x_1 - a_1, \ldots, x_d - a_d)$, so $Z(\mathfrak{m}) = \{(a_1, \ldots, a_d)\}$; in particular, it is nonempty. □

To attack the main question, we will need an observation on inequations. Observe that, if $f(\underline{x})$ is a polynomial, $f(\underline{a}) \neq 0$ if and only if there is a solution $y = b \in K$ to $yf(\underline{a}) - 1 = 0$. In particular, a system of polynomial equations and inequations

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

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

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

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

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

Theorem 2.16 (Strong Nullstellensatz)**.** *Let K be an algebraically closed field, and $R = K[x_1, \ldots, x_d]$ be a polynomial ring. Let $I \subseteq R$ be an ideal. The polynomial f vanishes on $Z_K(I)$ if and only if $f^n \in I$ for some $n \in \mathbb{N}$.*

Proof. If $f^n \in I$, and $\underline{a} \in Z_K(I)$, then $f(\underline{a}) \in K$ satisfies $f(\underline{a})^n = 0 \in K$. Since K is a field, $f(\underline{a}) = 0$. Thus, $f \in Z_K(I)$ as well.

Suppose that $f(\underline{x})$ vanishes along $Z_K(I)$. By the discussion above, this implies that $Z_K(I + (yf - 1)) = \varnothing$, in a polynomial ring in one more variable. By the Medium Nullstellensatz, we see that $1 \in IR[y] + (yf - 1)$. Write $I = (g_1(\underline{x}), \ldots, g_m(\underline{x}))$, 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 map y to $1/f$ to get

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

in the fraction field of $R[y]$. 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 multiply by f^n to obtain (on the LHS) f^n as a polynomial combination of the g's (on the RHS). □

Definition 2.17. *The* radical *of an ideal I is the ideal $\sqrt{I} := \{f \in R \mid \exists n : f^n \in I\}$. 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 $(rf)^m = r^m f^m \in I$.

Exercise 2.18. If R is a ring and I an ideal, then R/I is *reduced* (has no nonzero nilpotents) if and only if I is a radical ideal.

In this terminology, the Strong Nullstellensatz asserts that, if $K = \overline{K}$, $Z_K(I) \subseteq Z_K(f)$ if and only if $f \in \sqrt{I}$.

Observe that $Z_K(\sqrt{J}) = Z_K(J)$ whether or not K is algebraically closed: "$\subseteq$" is clear, and if $f^n(\underline{a}) = 0$, then $f(\underline{a}) = 0$, so $\underline{a} \in Z_K(J)$ and $f \in \sqrt{J}$ implies $f(\underline{a}) = 0$, and the equality of sets follows.

Definition 2.19. *If K is an algebraically closed field, and $X \subseteq K^n$ is a subset of the form $X = Z_K(I)$ for some (radical) ideal $I \subseteq K[x_1, \ldots, x_n]$, then we call X an* affine variety*, or a* subvariety of K^n*.*

Corollary 2.20. *Let K be an algebraically closed field, and $R = K[x_1, \ldots, x_d]$ a polynomial ring. There is an order-reversing bijection between the collection of subvarieties of K^d and the collection*

of radical ideals of R:

$$\begin{array}{lcl} \{\text{subvarieties of } K^d\} & \leftrightarrow & \{\text{radical ideals } I \subseteq R\} \\ X & \overset{\mathcal{I}}{\mapsto} & \{f \in R \mid X \subseteq Z_K(f)\} \\ Z_K(I) & \overset{\mathcal{Z}}{\mapsfrom} & I. \end{array}$$

In particular, for two ideals I, J, $Z_K(I) = Z_K(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Proof. We check that $\mathcal{I}$ and $\mathcal{Z}$ are inverse operations on the specified sets; namely that $\mathcal{Z}(\mathcal{I}(X)) = X$ for any subvariety X, and $\mathcal{I}(\mathcal{Z}(J)) = J$ for any radical ideal J.

The Strong Nullstellensatz says that $\mathcal{I}(\mathcal{Z}(J)) = \sqrt{J}$ for any ideal J, hence $\mathcal{I}(\mathcal{Z}(J)) = J$ for a radical ideal J.

Given X we can write $X = Z_K(J)$ for some radical ideal J. Then $\mathcal{Z}(\mathcal{I}(X)) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(J))) = \mathcal{Z}(J) = X$. □

Definition 2.21. *Let K be an algebraically closed field, and $X = Z_K(I) \subseteq K^d$ be a subvariety of K^d. The* coordinate ring *of X is the ring $K[X] := K[x_1, \ldots, x_d]/\mathcal{I}(X)$.*

Since $K[X]$ is obtained from the polynomial ring on the ambient K^d by quotienting out by exactly those polynomials that are zero on X, we interpret $K[X]$ as the ring of polynomial functions on X. Note that every reduced finitely generated K-algebra is a coordinate ring of some zeroset X, and conversely.

We now want to discuss maps on the set of maximal ideals. We prepare with a lemma.

Lemma 2.22. *Let $R \subseteq S$ be an integral extension.*

1. *Every nonzero element of S has a nonzero S-multiple in R.*
2. *If R is a field and S is a domain, then S is a field.*

Proof. 1. Let $s \in S$. Take an integral equation of dependence for s over R with lowest degree:

$$s^n + r_1 s^{n-1} + \cdots + r_n = 0.$$

WLOG, $r_n \neq 0$, otherwise we could take an integral equation of lower degree. Rewriting, we have $r_n = s(-s^{n-1} - r_1 s^{n-1} - \cdots - r_{n-1}) \in R$, as required.

2. Given $r \in R \smallsetminus 0$, there is some $s \in R$ such that $k = rs \in K \smallsetminus 0$. Then sk^{-1} is an inverse for r.

□

Proposition 2.23. *Let K be a field, and $\varphi : R \to S$ be a map of finitely generated K-algebras. Then, for any maximal ideal $\mathfrak{n}$ of S, $\mathfrak{m} = \varphi^{-1}(\mathfrak{n})$ is a maximal ideal of R.*

Proof. The map $K \subseteq S/\mathfrak{n}$ is module-finite, hence the intermediate extension $K \subseteq R/\varphi^{-1}(\mathfrak{n})$ is module-finite as well. Since $R/\varphi^{-1}(\mathfrak{n}) \subseteq S/\mathfrak{n}$, it is a domain. By the previous lemma, $R/\varphi^{-1}(\mathfrak{n})$ is a field. □

3 Septiembre

2.4 The prime spectrum of a ring

We have seen that the set of maximal ideals in a (reduced) finitely generated algebra over an algebraically closed field is bijective to a subset of K^n for some n.

We can carry more of the geometric information on this set of maximal ideals by giving it a topology. The *Zariski topology* on K^n is the topology whose closed sets are zero sets of polynomial equations, equivalently, $Z_K(I)$ for the ideals $I \subseteq K[x_1, \ldots, x_n]$. In light of the Nullstellensatz, we can generalize this construction to all rings.

The *maximal spectrum* of a ring R, denoted $\mathrm{Max}(R)$, is the set of maximal ideals of R endowed with the topology with closed sets given by $V_{\mathrm{Max}}(I) := \{\mathfrak{m} \in \mathrm{Max}(R) \mid \mathfrak{m} \supseteq I\}$ as I varies. By the Nullstellensatz, for polynomial rings S over an algebraically closed field K, this space $\mathrm{Max}(S)$ has a natural homeomorphism to K^n with its Zariski topology, and for an ideal I and S as above, $\mathrm{Max}(S/I)$ has a natural homeomorphism to $Z_K(I) \subseteq K^n$ with the subspace topology coming from the Zariski topology. Moreover, this is functorial: for any map of finitely generated K-algebras, there is an induced map on maximal ideals.

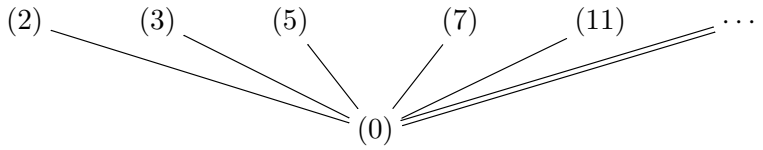
This is not quite the right notion to deal with general rings, for at least two reasons. First, there are many many interesting rings with only one maximal ideal! Second, we would like to have a geometric space that is assigned *functorially* to a ring, meaning that ring homomorphisms induce continuous maps of spaces (in the other direction). For the inclusion $A = K[x, y] = K[x-1, y]$ into $B = K(x)[y] = K(x-1)[y]$, what maximal ideal in A would we assign to $(y) \subseteq B$? How could one of (x, y) or $(x-1, y)$ have a better claim than the other?

Definition 2.24. *Let R be a ring. The* prime spectrum*, or* spectrum *of R is the set of prime ideals of R, denoted* $\mathrm{Spec}(R)$*. It is naturally a poset, partially ordered by inclusion. We also endow it with the topology with closed sets $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}$ for ideals $I \subseteq R$ (and $\varnothing = V(I)$ is closed).*

We will justify that this forms a topology shortly.

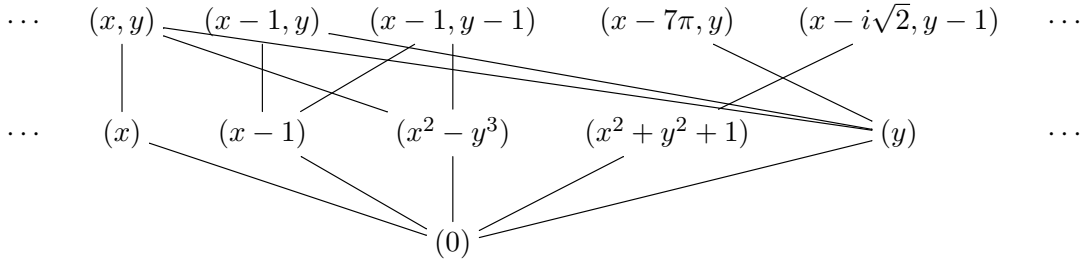
We will illustrate posets with Hasse diagrams: if an element is below something with a line connecting them, the higher element is $\geq$ the lower one.

Example 2.25. 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.

Example 2.26. Here are a few elements in $\mathbb{C}[x, y]$:



Note that $\mathrm{Max}(R)$ is a subspace of $\mathrm{Spec}(R)$ (that may be neither closed nor open).

Proposition 2.27. *Let R be a ring, and I_λ, J be ideals (possibly improper).*

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. *$\mathrm{Spec}(R)$ has a basis given by open sets of the form $D(f) := \mathrm{Spec}(R) \smallsetminus V(f)$.*
5. *$\mathrm{Spec}(R)$ is quasicompact.*

Proof. 1. Clear.

2. 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.

3. Clear.

4. We can write any open set as the complement of $V(\{f_\lambda\}) = \bigcap_\lambda V(f_\lambda)$, which is the union of $D(f_\lambda)$.

5. Given a sequence of ideals I_λ,if $\sum_\lambda I_\lambda = R$, then 1 is in the sum on the left, and thus 1 can be realized in such a sum over finitely many indices: $\sum_\lambda I_\lambda = I_{\lambda_1} + \cdots + I_{\lambda_t}$. Thus, if we have a family of closed sets with empty intersection,

$$\varnothing = \bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda) = V(I_{\lambda_1} + \cdots + I_{\lambda_t}) = V(I_{\lambda_1}) \cap \cdots \cap V(I_{\lambda_t}),$$

so some finite subintersection is empty. □

Definition 2.28 (Induced map on Spec)**.** *Given a homomorphism of rings $\varphi : R \to S$, we obtain a map on spectra $\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ given by $\varphi^*(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$.*

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

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

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

Example 2.29. Let $\pi : R \to R/I$ be surjective. Then the map $\pi^* : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ corresponds to the inclusion of $V(I)$ into $\mathrm{Spec}(R)$, since primes of R/I correspond to primes of R containing I.

We can use the spectrum of a ring to give an analogue of the strong Nullstellensatz that is valid for any ring. To prepare for this, we need a notion that we will use later.

Definition 2.30. *A subset $W \subseteq R$ of a ring R is* multiplicatively closed *if $1 \in W$ and $a, b \in W \Rightarrow ab \in W$.*

Lemma 2.31. *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. □

5 Septiembre

Proposition 2.32 (Spectrum analogue of strong Nullstellensatz)**.** *Let R be a ring, and I be an ideal. For $f \in R$,*

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

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

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. □

The following corollary follows in exactly the same way as the analogous statement for subvarieties of K^n, Corollary 2.20.

Corollary 2.33. *Let R a ring. There is an order-reversing bijection*

$$\{\textit{closed subsets of } \operatorname{Spec}(R)\} \qquad \leftrightarrow \qquad \{\textit{radical ideals } I \subseteq R\}.$$

In particular, for two ideals I, J, $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Chapter 3

Exact functors, localization, flatness

3.1 Exact, left-exact, right-exact sequences

Definition 3.1. *A sequence of maps of R-modules*

$$\cdots \to M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{t-1}} M_t \to \cdots$$

is said to be exact *if for all $1 < i < t$, one has $\ker(\alpha_i) = \operatorname{im}(\alpha_{i-1})$ as submodules of M_i. We allow sequences that may or may not continue indefinitely in either direction.*

For a while, we will be happy to focus on a few special cases.

Definition 3.2. *A* short exact sequence *of R-modules is an exact sequence of the form*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0;$$

that is:

- $\ker(\alpha) = 0$*; i.e., α is injective,*
- $\operatorname{coker}(\beta) = 0$*; i.e., β is surjective, and*
- $\ker(\beta) = \operatorname{im}(\alpha)$.

Since α is injective, $L \cong \alpha(L)$. If we identify L with $\alpha(L)$, then the data of the short exact sequence above translates to $N \cong M/L$, with $\alpha : L \to M$ the inclusion map, and $\beta : M \to N$ to quotient map.

Definition 3.3. *A* right exact sequence *of R-modules is an exact sequence of the form*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0;$$

that is:

- $\operatorname{coker}(\beta) = 0$*; i.e., β is surjective, and*
- $\ker(\beta) = \operatorname{im}(\alpha)$.

The data of a right exact sequence translates to $N \cong \operatorname{coker}(\alpha) = M/\operatorname{im}(\alpha)$, with $\beta : M \to N$ the quotient map from the target onto the cokernel.

A special case of this is when M and N are free.

Definition 3.4. *A* presentation *of a module N is a right-exact sequence of the form*

$$F_1 \xrightarrow{\alpha} F_0 \to N \to 0$$

with F_1 and F_0 free.

The image of the free basis of F_0 in N is a generating set for N; this is equivalent to surjectivity. The image of F_1 in F_0 gives the *relations* on those generators.

Remark 3.5. We say that a module is *finitely presented* or *finitely presentable* if it admits a presentation by finitely generated free modules. If R is Noetherian, then finitely generated and finitely presented are equivalent.

Definition 3.6. *A* left exact sequence *of R-modules is an exact sequence of the form*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N;$$

that is:

- $\ker(\alpha) = 0$*; i.e., α is injective, and*
- $\ker(\beta) = \mathrm{im}(\alpha)$.

The data of a left exact sequence translates to $L \cong \ker(\beta)$, and $\alpha : L \to M$ is the inclusion of the kernel into the source.

Observe that a sequence of maps $0 \to L \to M \to N \to 0$ is short exact if and only if it is left and right exact.

3.2 Hom and projectives

Definition 3.7. *Let L, M, N be R-modules.*

- *The* module of homomorphisms *from M to N is*

  $$\mathrm{Hom}_R(M, N) := \{\phi : M \to N \mid \phi \text{ is } R\text{-linear}\}.$$

  The R-module structure is given by the rule $r \cdot \phi$ is the homomorphism $m \mapsto r\phi(m) = \phi(rm)$.

- *If $\alpha : M \to N$ is a module homomorphism, we define a map $\mathrm{Hom}_R(L, \alpha)$ or α_* from $\mathrm{Hom}_R(L, M) \to \mathrm{Hom}_R(L, N)$ by the rule*

  $$\alpha_*(\phi) = \alpha \circ \phi;$$

  i.e.,

  $$\alpha_* : \quad (\ L \xrightarrow{\phi} M\ ) \quad \mapsto \quad (\ L \xrightarrow{\alpha} M \xrightarrow{\phi} N\ ).$$

- *If $\alpha : M \to N$ is a module homomorphism, we define a map $\mathrm{Hom}_R(\alpha, L)$ or α^* from $\mathrm{Hom}_R(N, L) \to \mathrm{Hom}_R(M, L)$ by the rule*

  $$\alpha^*(\phi) = \phi \circ \alpha;$$

  i.e.,

  $$\alpha^* : \quad (\ N \xrightarrow{\phi} L\ ) \quad \mapsto \quad (\ M \xrightarrow{\alpha} N \xrightarrow{\phi} L\ ).$$

Thus, given a fixed R-module L, $F(-) := \mathrm{Hom}_R(L, -)$ is a rule that assigns to any R-module M another R-module $F(M)$, and to any homomorphism $M \xrightarrow{\phi} N$ a homomorphism $F(M) \xrightarrow{F(\phi)} F(N)$. This (plus the fact that F takes the identity map to the identity map and compositions to compositions) makes F a *covariant functor* from R-modules to R-modules.

Similarly, given a fixed R-module L, $G(-) := \mathrm{Hom}_R(-, L)$ is rule that assigns to any R-module M another R-module $G(M)$, and to any homomorphism $G(M) \xrightarrow{\phi} G(N)$ a homomorphism $G(N) \xrightarrow{G(\phi)} G(M)$. This (with the same caveats as above) makes G a *contravariant functor* from R-modules to R-modules. The covariant vs. contravariant bit refers to whether the directions of maps have changed.

Given maps $L \xrightarrow{\alpha} L'$ and $M \xrightarrow{\beta} M'$, we likewise get a map $\mathrm{Hom}_R(L', M) \xrightarrow{\mathrm{Hom}_R(\alpha,\beta)} \mathrm{Hom}_R(L, M')$, by combining the constructions above.

Example 3.8. $\mathrm{Hom}_R(R, M) \cong M$ by $\phi \mapsto \phi(1)$, and under this isomorphism, $M \xrightarrow{\alpha} N$ corresponds to $1 \mapsto m \rightsquigarrow 1 \mapsto \alpha(m)$ under this isomorphism.

If I is an ideal, $\mathrm{Hom}_R(R/I, M) \cong \mathrm{ann}_M(I)$ by the same map: the image of 1 in R/I must map to something killed by I, and there is a unique R-linear map that does this. The same recipe for maps as above holds. Thus, we can identify $\mathrm{Hom}_R(R/I, -)$ with the functor that sends modules M to $\mathrm{ann}_M(I)$, and sends maps to their restrictions to these submodules.

Theorem 3.9. *1. A sequence of maps*

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

is left-exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(X, L) \xrightarrow{\alpha_*} \mathrm{Hom}_R(X, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(X, N)$$

is left-exact.

2. A sequence of maps

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is right-exact if and only if, for all R-modules X, the sequence

$$0 \to \mathrm{Hom}_R(N, X) \xrightarrow{\beta^*} \mathrm{Hom}_R(M, X) \xrightarrow{\alpha^*} \mathrm{Hom}_R(L, X)$$

is left-exact.

Proof. Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ be left-exact, and X be an R-module.

- α_* is injective: if $X \xrightarrow{\phi} L$ is nonzero, $X \xrightarrow{\phi} L \xrightarrow{\alpha} M$ is as well, since a nonzero element in the image of ϕ goes to something nonzero in the composition.
- $\ker(\beta_*) = \mathrm{im}(\alpha_*)$: $X \xrightarrow{\phi} M \xrightarrow{\beta} N$ is zero if and only if $\mathrm{im}(\phi) \subseteq \ker(\beta) = \mathrm{im}(\alpha)$, which happens if and only if ϕ factors through L; i.e., $\phi \in \mathrm{im}(\alpha_*)$.

The other direction of the first part follows from the example above; we can use $X = R$.

Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a right-exact sequence, and X be an R-module.

- β^* is injective: if $N \xrightarrow{\phi} X$ is nonzero, pick $n \in N$ not in the kernel, and $m \in M$ that maps to n. Then, the image of m under $M \xrightarrow{\beta} N \xrightarrow{\phi} X$ is nonzero.
- $\ker(\alpha^*) = \operatorname{im}(\beta_*)$: $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero if and only if $\operatorname{im}(\alpha) \subseteq \ker(\phi)$, which happens if and only if ϕ descends to a map of the form $N \cong M/\operatorname{im}(\alpha) \to X$; i.e., $\phi \in \operatorname{im}(\alpha^*)$.

Let $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a sequence of maps, and suppose that it is exact after applying $\operatorname{Hom}_R(-, X)$ for all X.

- β is surjective: if not, let $X = N/\operatorname{im}(\beta)$. There is a nonzero projection map $N \xrightarrow{\phi} X$, but $M \xrightarrow{\beta} N \xrightarrow{\phi} X$ is zero, contradicting injectivity of β^*.
- $\ker(\beta) \supseteq \operatorname{im}(\alpha)$: Take $X = N$, and $N \xrightarrow{\mathrm{id}} X$. Since $\ker(\alpha^*) \supseteq \operatorname{im}(\beta^*)$, $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \xrightarrow{\mathrm{id}} X = L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is zero.
- $\ker(\beta) \subseteq \operatorname{im}(\alpha)$: Take $X = M/\operatorname{im}(\alpha)$, and $M \xrightarrow{\phi} X$ the projection map. Since $L \xrightarrow{\alpha} M \xrightarrow{\phi} X$ is zero, ϕ is in the image of β^*, so it factors through β. This is equivalent to the stated containment. □

In short, $\operatorname{Hom}_R(X, -)$ is kernel-preserving, and $\operatorname{Hom}_R(-, X)$ turns cokernels into kernels.

10 Septiembre

Definition 3.10. *An R-module is projective P if the functor $\operatorname{Hom}_R(P, -)$ sends short exact sequences to short exact sequences. Equivalently, P is projective if $M \xrightarrow{\alpha} N$ surjective implies $\operatorname{Hom}_R(P, M) \xrightarrow{\operatorname{Hom}(P,\alpha)} \operatorname{Hom}_R(P, N)$ is surjective.*

Free modules are always projective: $\operatorname{Hom}_R(R^{\oplus\Gamma}, M) \cong M^{\oplus\Gamma}$, and a map α gets sent to Γ copies of itself. Every projective module is a direct summand of a free module: we can map a free module F onto P, and since $\operatorname{Hom}_R(P, F) \twoheadrightarrow \operatorname{Hom}_R(P, P)$, the identity map of P is in the image: the identity factors through F. Every direct summand of a free module is projective as well (exercise!).

Example 3.11. Let $R = S \times T$ be a direct product of rings. Then $S(= S \times 0)$ is a direct summand of R as an R-module: writing π for the projection, we have $\pi((s,t)(s',0)) = \pi((ss',0)) = (ss',0) = (s,t)\pi((s',0))$; but is not free, since a free generator would have annihilator zero, but every element of S is annihilated by T. Thus not every projective module is free.

3.3 Tensor products and flat modules

Definition 3.12. *Let M and N be R-modules. The tensor product of M and N is the module $M \otimes_R N$ generated by the set $\{m \otimes n \mid m \in M, n \in N\}$ with relations*

$$(rm + m') \otimes n - r(m \otimes n) - m' \otimes n \qquad m, m' \in M, n \in N, r \in R$$
$$m \otimes (rn + n') - r(m \otimes n) - m \otimes n' \qquad m \in M, n, n' \in N, r \in R.$$

Observe that if $M = \sum_\alpha Rm_\alpha$ and $N = \sum_\beta Rn_\beta$, then $M \otimes_R N = \sum_{\alpha,\beta} m_\alpha \otimes n_\beta$: any element is a sum of elements of the form $m \otimes n$, and using the relations above, we can write any $m \otimes n$ as a linear combination of the specified generators. In particular, the tensor product of two finitely generated modules is finitely generated.

Tensor products are characterized by a universal property.

Definition 3.13. *Let L, M, N be R-modules. A map $\varphi : M \times N \to L$ is* bilinear *over R if it is linear in both the M and N arguments: $\varphi(rm + m', n) = r\varphi(m, n) + \varphi(m', n)$ and $\varphi(m, rn + n') = r\varphi(m, n) + \varphi(m, n')$. We write $\mathrm{Bil}_R(M, N; L)$ for the set of bilinear maps $M \times N \to L$.*

Like Hom, Bil is an R-module, defined by the action of R on any of the inputs.

The following follows from the definition.

Proposition 3.14. *Let L, M, N be R-modules. There is a bilinear map of R-modules $\rho : M \times N \to M \otimes_R N$ such that for any bilinear map $\varphi : M \times N \to L$, there is a unique R-module homomorphism $\phi : M \otimes_R N \to L$ with $\varphi = \phi \circ \rho$. This map ρ is given by $\rho(m, n) = m \otimes n$.*

Consequently, there is an R-module isomorphism $\mathrm{Hom}_R(M \otimes_R N, L) \cong \mathrm{Bil}_R(M, N; L)$.

Proof. With φ fixed, we observe that if an R-linear map ϕ with $\varphi = \phi \circ \rho$ exists, then $\phi(m \otimes n) = \varphi(m, n)$ for all simple tensors $m \otimes n$; since these generate, this determines the map completely, if it exists. To see the existence, we consider the map on the free module F generated by the symbols $m \otimes n$ (with no relations) given by $m \otimes n \mapsto \varphi(m, n)$. Using the biliearity relations on φ, we see that all elements of the form $(rm+m') \otimes n - r(m \otimes n) - m' \otimes n$ and $m \otimes (rn+n') - r(m \otimes n) - m \otimes n'$ must map to zero, so the map factors through the tensor product. □

Here are some consequences of this universal property.

Proposition 3.15. *Let L, M, M_λ, N be R-modules.*

1. *$R \otimes_R M \cong M$.*
2. *$M \otimes_R N \cong N \otimes_R M$.*
3. *$(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N)$.*
4. *$(\bigoplus_{\lambda \in \Lambda} M_\lambda) \otimes_R N \cong \bigoplus_{\lambda \in \Lambda} (M_\lambda \otimes_R N)$.*
5. *If S is an R-algebra, and N is an S-module, $M \otimes_R (S \otimes_S N) \cong M \otimes_R N$.*

Proof. We prove a few, and leave the rest for you to verify or check in a difference source.

For #1, there is a bilinear map $R \times M \to M$ given by $(r, m) \mapsto rm$, which induces a map $R \otimes_R M \to M$ sending $r \otimes m \mapsto m$. The map $\phi : M \to R \otimes M$ given by $r \mapsto 1 \otimes m$ is R-linear: $\phi(rm + m') = 1 \otimes (rm + m') = r(1 \otimes m) + (1 \otimes m') = r\phi(m) + \phi(m')$, so the maps are mutually inverse R-module homomorphisms.

For #2, there is a bilinear map $M \times N \to N \otimes_R M$ given by $(m, n) \mapsto n \otimes m$, which induces a map $M \otimes_R N \to N \otimes_R M$ sending $m \otimes n \mapsto n \otimes m$. An inverse is constructed in a similar way. □

Definition 3.16. *If $L \xrightarrow{\alpha} L'$ is a map of R-modules, and M is another R-module, there is an R-module homomorphism $L \otimes_R M \xrightarrow{\alpha \otimes M} L' \otimes_R M$ given by $(\alpha \otimes M)(l \otimes m) = \alpha(l) \otimes m$ on simple tensors. This is the map coming from the universal property applied to $L \times M \xrightarrow{\alpha \times \mathrm{id_M}} L' \times M \to L' \otimes_R M$.*

Likewise, given two maps $L \xrightarrow{\alpha} L'$, $M \xrightarrow{\beta} M'$, there is a map $L \otimes_R M \xrightarrow{\alpha \otimes \beta} L' \otimes_R M'$.

Thus, if N is an R-module, $- \otimes_R N$ is a covariant functor.

Theorem 3.17 (Hom-tensor adjointness)**.** *Let L, M, N be R-modules. There is an isomorphism $\mathrm{Hom}_R(L \otimes_R M, N) \cong \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$. These isomorphisms are functorial in each argument (i.e., are natural transformations of functors of each argument L, M, N).*

Proof. (Sketch) We have that $\mathrm{Hom}_R(L \otimes_R M, N) \cong \mathrm{Bil}(L, M; N)$ via the rule $(L \otimes_R M \to N) \mapsto (L \times M \xrightarrow{\rho} L \otimes_R M \to N)$. We claim that $\mathrm{Bil}_R(L, M; N) \cong \mathrm{Hom}_R(L, \mathrm{Hom}_R(M, N))$ by the map sending $\phi \mapsto (x \mapsto \phi(x, -))$; the inverse is $\psi \mapsto ((x, y) \mapsto \psi(x)(y))$. □

Theorem 3.18. *If a sequence of maps*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$$

is right-exact, then

$$L \otimes_R X \xrightarrow{\alpha \otimes X} M \otimes_R X \xrightarrow{\beta \otimes X} N \otimes_R X (\to 0)$$

is right-exact.

Proof. To see that the latter sequence is right-exact, we show that if we apply $\mathrm{Hom}_R(-, Y)$ to it, it yields a left-exact sequence, for all R-modules Y. The sequence becomes

$$\begin{array}{ccccc} \mathrm{Hom}_R(N \otimes X, Y) & \xrightarrow{\mathrm{Hom}(\beta \otimes X, Y)} & \mathrm{Hom}_R(M \otimes X, Y) & \xrightarrow{\mathrm{Hom}(\alpha \otimes X, Y)} & \mathrm{Hom}_R(L \otimes X, Y) \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ \mathrm{Hom}_R(N, \mathrm{Hom}_R(X, Y)) & \xrightarrow{\mathrm{Hom}(\beta, \mathrm{Hom}(X, Y))} & \mathrm{Hom}_R(M, \mathrm{Hom}_R(X, Y)) & \xrightarrow{\mathrm{Hom}(\alpha, \mathrm{Hom}(X, Y))} & \mathrm{Hom}_R(L, \mathrm{Hom}_R(X, Y)). \end{array}$$

It follows from left-exactness of Hom that the bottom row is left-exact, so the top row must be as well. □

Remark 3.19. Let S be an R-algebra. If M is an R-module, then $S \otimes_R M$ is an S-module, where S acts on the S-factor. If $M \xrightarrow{\alpha} N$ is a map of R-modules, then $S \otimes_R M \xrightarrow{S \otimes \alpha} S \otimes_R N$ is a map of S-modules. The functor $S \otimes_R -$ is called *extension of scalars* from R to S.

Observe that $S \otimes R^{\oplus \Lambda} \cong S^{\oplus \Lambda}$ as S-modules. By right-exactness, it follows that extension of scalars preserves presentations. That is, if

$$R^m \xrightarrow{A} R^n \to M \to 0$$

is a presentation, then

$$S^m \xrightarrow{A} S^n \to S \otimes_R M \to 0$$

is a presentation.

Definition 3.20 (Flat module)**.** *An R-module N is* flat *if, for any inclusion of modules $M' \hookrightarrow M$, the map $M' \otimes_R N \to M \otimes_R N$ is injective. Equivalently, N is flat if $- \otimes_R N$ preserves exact sequences.*

If $\phi : R \to S$ is a map of rings, we say that S is a flat R-algebra *or ϕ is a* flat homomorphism *if S is a flat R-module.*

Lemma 3.21. *Projective modules, and in particular, free modules, are flat.*

Proof. First, if F is free, then $\alpha \otimes_R F$ is a direct sum of copies of the map α, so is α is injective, then so is $\alpha \otimes_R F$.

Now, if P is projective, there are maps $P \xrightarrow{i} F \xrightarrow{p} P$ that compose to the identity. Thus $P \otimes_R N \xrightarrow{i\otimes_R N} F \otimes_R N \xrightarrow{p\otimes_R N} P \otimes_R N$ is the identity, so $P \otimes_R N \xrightarrow{i\otimes_R N} F \otimes_R N$ is always injective. For any injection $M' \to M$, we have a commutative diagram

$$\begin{array}{ccc} M' \otimes_R F & \longrightarrow & M \otimes_R F \\ \uparrow & & \uparrow \\ M' \otimes_R P & \longrightarrow & M \otimes_R P \end{array}$$

and since the diagonal is injective, $M' \otimes_R P \to M \otimes_R P$ must be injective. □

12 Septiembre

Lemma 3.22. *If $\phi : R \to S$ is a ring homomorphism, and M is a flat R-module, then $S \otimes_R M$ is a flat S-module.*

Proof. $(S \otimes_R M) \otimes_S N \cong M \otimes_R (S \otimes_S N) \cong M \otimes_R N$, and under this identification, $(S \otimes_R M) \otimes_S \alpha$ agrees with $M \otimes_R \alpha$. □

Proposition 3.23 (Equational criterion)**.** *If M is flat, the following condition holds:*

For any $\underline{r} = (r_1, \dots, r_t) \in R^t$ and $\underline{m} = (m_1, \dots, m_t) \in M^t$ with $\underline{r} \cdot \underline{m} = 0$, there exist $\underline{s}_j = (s_{1j}, \dots, s_{tj}) \in R^t$ for $j = 1, \dots, a$ such that $\underline{r} \cdot \underline{s}_j = 0$ and $n_1, \dots, n_a \in M$ such that $\underline{m} = \sum_{j=1}^{a} \underline{s}_j n_j$.

Proof. Let M be flat. Given a t-tuple of elements $\underline{r} \in R^t$, consider the exact sequence $0 \to K \to R^t \xrightarrow{[\underline{r}]} R$, where K is the kernel. By assumption, $0 \to K \otimes_R M \to M^t \xrightarrow{[\underline{r}]} M$ is exact. That is,

$$\underline{r} \cdot \underline{m} = 0 \Rightarrow \underline{m} \in \ker([\underline{r}]) \Rightarrow \underline{m} \in K \otimes_R M.$$

Thus, such an $\underline{m}$ can be written as $\sum_j k_j \otimes n_j$ for some $k_j \in K$ and $n_j \in M$. Unpackaging the definitions gives the elements we want. □

Example 3.24. Suppose that r is a nonzerodivisor on R: $ry = 0 \Rightarrow y = 0$ for $y \in R$. If M is a flat module, x is a nonzerodivisor on M. Indeed, $rm = 0$ implies that there are $s_1, \dots, s_j \in R$ such that $rs_j = 0$ for each j and $m \in (s_1, \dots, s_j)M$, but all $s_j = 0$ by hypothesis, so $m = 0$.

Another useful fact:

Proposition 3.25 (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*

$$\begin{array}{rcl} S \otimes_R \mathrm{Hom}_R(M, N) & \cong & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\ s \otimes \varphi & \mapsto & s(S \otimes \varphi) \end{array}$$

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 $\mathrm{Hom}_S(-, S \otimes_R N)$ to this presentation, we obtain a left-exact sequence

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

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

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

We then have a diagram

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

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 $\to$ to $s \cdot (S \otimes (\varphi \circ \alpha))$, whereas $s \otimes \varphi$ goes $\to$ 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. □

We want to briefly note a definition related to flatness.

Definition 3.26 (Faithfully flat module)**.** *A module N over a ring R is* faithfully flat *if $L \xrightarrow{\alpha} M$ is injective if and only if $L \otimes_R N \xrightarrow{\alpha\otimes N} M \otimes_R N$ is injective.*

We can talk of faithfully flat algebras / morphisms as with flat algebras / morphisms.

Proposition 3.27. *Let M be a faithfully flat R-module, and S an R-algebra. Then $M \otimes_R S$ is faithfully flat over S. In particular, if R is a K-algebra, and L is an extension field of K, then $R \otimes_K L$ is faithfully flat over R.*

3.4 Localization

Recall the notion of multiplicative set.

Our three most important classes of examples are the first three below.

Example 3.28. 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 $W = R \setminus \mathfrak{p}$ 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.

4. An arbitrary intersection of multiplicatively closed subsets is multiplicatively closed. In particular, for any family of primes $\{\mathfrak{p}_\lambda\}$, the set $R \smallsetminus \bigcup_\lambda \mathfrak{p}_\lambda$ is multiplicatively closed.

Definition 3.29 (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

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

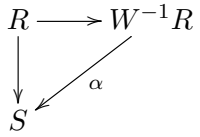
There is a canonical ring homomorphism $R \to W^{-1}R$ that sends $r \mapsto \frac{r}{1}$.

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.

In the localization of R at W, every element of W becomes a unit. The following universal property says roughly that $W^{-1}R$ is the smallest R-algebra in which every element of R is a unit.

Proposition 3.30. *Let R be a ring, and W a multiplicative set with $0 \notin W$. Let S be an R-algebra in which every element of W is a unit. Then there is a unique homomorphism α such that the following diagram commutes:*



where the vertical map is the structure homomorphism and the horizontal map is the canonical homomorphism.

Example 3.31 (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 3.32. *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 3.33. *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 3.34. 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 3.35. *Let M be a module, and $N_1, \ldots, N_t$ 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. □

17 Septiembre

Theorem 3.36 (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.*

Proof. 1. The bilinear map $W^{-1}R \times M \to W^{-1}M$ given by $(r/w, m) \mapsto rm/w$ induces a map ψ from the tensor product that is clearly surjective. For an inverse map, set $\phi(m/w) = 1/w \otimes m$. To see this is well-defined, suppose $m/w = m'/w'$, so $\exists v \in W$ such that $v(mw' - m'w) = 0$. Then,

$$\phi(m/w) - \phi(m'/w') = 1/w \otimes m - 1/w' \otimes m'.$$

We can multiply through by vww'/vww' to get

$$\frac{vw'}{vww'} \otimes m - \frac{vw}{vww'} \otimes m' = \frac{1}{vww'} \otimes v(mw' - m'w) = 0.$$

To see this is a homomorphism, we note that

$$\begin{aligned}\phi(\frac{m}{w} + \frac{m'}{w'}) = \phi(\frac{mw' + m'w}{ww'}) = \frac{1}{ww'} \otimes (mw' + m'w) = \frac{1}{ww'} \otimes mw' + \frac{1}{ww'} \otimes m'w \\ = \frac{w'}{ww'} \otimes m + \frac{w}{ww'} \otimes m' = \frac{1}{w} \otimes m + \frac{1}{w'} \otimes m' = \phi(\frac{m}{w}) + \phi(\frac{m'}{w'}),\end{aligned}$$

and

$$\phi(r\frac{m}{w}) = \frac{1}{w} \otimes rm = r(\frac{1}{w} \otimes m) = r\phi(\frac{m}{w}).$$

The composition $\phi \circ \psi$ sends $r/w \otimes m \mapsto rm/w \mapsto 1/w \otimes rm = r/w \otimes m$; since it is the identity on simple tensors and additive, it is the identity.

For the claim about maps, we need to see that, for $M \xrightarrow{\alpha} N$, we have to check $\psi_N \circ (W^{-1}R \otimes \alpha) = W^{-1}\alpha \circ \psi_M$. Indeed,

$$\begin{aligned}(\psi_N \circ (W^{-1}R \otimes \alpha))(\frac{r}{w} \otimes m) = \psi_N(\frac{r}{w} \otimes \alpha(m)) = \frac{r\alpha(m)}{w} \\ = \frac{\alpha(rm)}{w} = W^{-1}\alpha(\frac{rm}{w}) = (W^{-1}\alpha \circ \psi_M)(\frac{r}{w} \otimes m).\end{aligned}$$

2. This follows from the earlier observation that $W^{-1}(-)$ preserves injective maps.

3. This is immediate from part (2). □

Corollary 3.37 (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,*

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

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

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

Proposition 3.38. *Let M be an R-module, and W a multiplicative set. Set $M_W = \{m \in M \mid \exists w \in W : wm = 0\}$ and $\overline{M} = M/M_W$. Then,*

$$W^{-1}M = \bigcup_{w \in W} \frac{1}{w}\overline{M},$$

where each $\frac{1}{w}\overline{M}$ is an isomorphic copy of $\overline{M}$ as an R-module.

Proof. First, M_W is a submodule of M and consists of the elements that go to zero in the localization. We have $W^{-1}\overline{M} \cong W^{-1}(M/M_W) \cong \frac{W^{-1}M}{W^{-1}M_W} \cong W^{-1}M$, so we can replace M by the W-torsionfree module $\overline{M}$. It is clear that every element of $W^{-1}M$ has the form on the RHS. The map $\overline{M} \to \frac{1}{w}\overline{M}$ sending $m \mapsto \frac{m}{w}$ is clearly R-linear, and is injective by the W-torsion free assumption. □

Proposition 3.39. *Let W be multiplicatively closed in 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.
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

$$\begin{array}{lcl} \operatorname{Spec}(W^{-1}R) & \leftrightarrow & S \\ \mathfrak{q} & \mapsto & \mathfrak{q} \cap R \\ W^{-1}\mathfrak{p} = \mathfrak{p}(W^{-1}R) & \leftarrow\!\shortmid & \mathfrak{p} \end{array}$$

   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 3.40. *Let R be a ring and $\mathfrak{p}$ be a prime ideal. The map $R \to R_{\mathfrak{p}}$ induces a map on spectra corresponding to the inclusion*

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

Definition 3.41. *Let $\phi : R \to S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. We call the ring*

$$\kappa_\phi(\mathfrak{p}) := (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$$

the fiber ring *of ϕ over $\mathfrak{p}$.*

The point of this definition is the following.

Lemma 3.42. *Let $\phi : R \to S$ be a ring homomorphism, and $\mathfrak{p} \in \operatorname{Spec}(R)$. $\operatorname{Spec}(\kappa_\phi(\mathfrak{p})) \cong (\phi^*)^{-1}(\mathfrak{p})$, the set of primes that contract to $\mathfrak{p}$.*

Proof. Consider the maps $S \to S/\mathfrak{p}S \to (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$. For the first map, the map on spectra can be identified with the inclusion of $V(\mathfrak{p}S)$ into $\operatorname{Spec}(S)$. For the second, it can be identified with the inclusion of the set of primes that do not intersect $R \smallsetminus \mathfrak{p}$, i.e., those whose contraction is contained in $\mathfrak{p}$. Put together, this is the set of primes that contract to $\mathfrak{p}$. □

Chapter 4

Decomposition of ideals

4.1 Minimal primes and support

We will consider a few ways of decomposing ideals into pieces, in three ways with increasing detail. The first is the most directly geometric: for any ideal I in a Noetherian ring, we aim to write $V(I)$ as a finite union of $V(\mathfrak{p}_i)$ for prime ideals $\mathfrak{p}_i$.

Definition 4.1. *The primes that contain I and are minimal with the property of containing I are called the* minimal primes *of I. That is, the minimial primes of I are the minimal elements of $V(I)$. We write* $\operatorname{Min}(I)$ *for this set.*

Lemma 4.2. *Let R be a ring, and I an ideal. Every prime $\mathfrak{p}$ that contains I contains a minimal prime of I. Consequently, $\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p} = \bigcap_{\mathfrak{p}\in \operatorname{Min}(I)} \mathfrak{p}$.*

Proof. This follows from Zorn's lemma. We just need to check that the intersection of a descending chain of prime ideals that contain I is prime and contains I. These are both trivial. The first equality in the "consequently" we already know; the second is basic set theory. □

Remark 4.3. If $\mathfrak{p}$ is prime, then $\operatorname{Min}(\mathfrak{p}) = \{\mathfrak{p}\}$. Also, we have $\operatorname{Min}(I) = \operatorname{Min}(\sqrt{I})$ (since $V(I) = V(\sqrt{I})$).

As a special case, the nilpotent elements of a ring R are exactly the elements in every minimal prime of R (equivalently, every minimal prime of the zero ideal).

Lemma 4.4. *Given an expression $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ with $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for each i, j, we have* $\operatorname{Min}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof. This boils down to the claim that if $\mathfrak{q}$ is prime, and $\mathfrak{q} \supseteq (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n)$ then $\mathfrak{q}$ contains some $\mathfrak{p}_i$. But, if $\mathfrak{q} \not\supseteq \mathfrak{p}_i$ for each i, there are elements $f_i \in \mathfrak{p}_i \smallsetminus \mathfrak{q}$, and the product $f_1 \cdots f_n \in (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n) \smallsetminus \mathfrak{q}$. □

Theorem 4.5. *Let R be a Noetherian ring. Then any ideal I has finitely many minimal primes, and thus, we can write*

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

Proof. Let $S = \{\text{ideals } I \subseteq R \mid \operatorname{Min}(I) \text{ is infinite}\}$, and suppose, to obtain a contradiction, that $S \neq \varnothing$. By Noetherianity, S has a maximal element J. Clearly, J is not prime (for $\operatorname{Min}(J)$ would be a singleton), but J is radical, since $\operatorname{Min}(J) = \operatorname{Min}(\sqrt{J})$. Partitioning the minimal primes of J into two nonempty sets we can write $J = J_1 \cap J_2$, where J_1 is the intersection of some of the

primes, and J_2 the intersection of the others, and $J \neq J_1, J_2$, since $V(J_1), V(J_2) \subsetneq V(J)$ and the ideals are radical. By choice of J, we know that $\mathrm{Min}(J_1)$ and $\mathrm{Min}(J_2)$ are finite. We then have $J_1 = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_a$ and $J_2 = \mathfrak{p}_{a+1} \cap \cdots \cap \mathfrak{p}_b$, where the $\mathfrak{p}_c's$ are minimal primes, so $J = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_b$. By the previous lemma, we see that $\mathrm{Min}(J)$ is a subset of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_b\}$, so is finite. □

19 Septiembre

We now can describe the relationship between the poset structure of $\mathrm{Spec}(R)$ and the topology.

Proposition 4.6. *Let R be a ring, and $X = \mathrm{Spec}(R)$.*

1. *The poset structure on X can be recovered from the topology by the rule: $\mathfrak{p} \subseteq \mathfrak{q}$ ($\mathfrak{p} \leq \mathfrak{q}$) $\Leftrightarrow$ $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$.*
2. *If R is Noetherian, the topology on X can by recovered from the poset structure by the rule*

$$Y \subseteq X \quad \textit{is closed} \quad \Leftrightarrow \quad \exists \mathfrak{p}_1, \ldots, \mathfrak{p}_n \in X : Y = \{\mathfrak{q} \in X \mid \mathfrak{p}_i \subseteq \mathfrak{q} \textit{ for some } i\}.$$

Proof. 1. We calculate the closure of a point. We have $\overline{\{\mathfrak{p}\}} = \bigcap_{\mathfrak{p} \in V(I)} V(I)$. Note that $\mathfrak{p} \in V(I)$ implies $I \subseteq \mathfrak{p}$, which implies $V(\mathfrak{p}) \subseteq V(I)$. It follows that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, and thus the claim.

2. If Y is closed, we have $Y = V(I) = V(\sqrt{I}) = V(\mathfrak{p}_1 \cap \cdots \mathfrak{p}_n) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_n)$. For the converse, we can work backwards. □

We now wish to understand modules in a similar way.

Definition 4.7. *If M is an R-module, the* support *of M is* $\mathrm{Supp}(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}$.

Proposition 4.8. *If R is a ring, and M a finitely generated module, then* $\mathrm{Supp}(M) = V(\mathrm{ann}_R(M))$. *In particular,* $\mathrm{Supp}(R/I) = V(I)$.

Proof. Let $M = \sum_i Rm_i$. We have that $\mathrm{ann}_R(M) = \bigcap_i \mathrm{ann}_R(m_i)$, so $V(\mathrm{ann}_R(M)) = \bigcup_i V(\mathrm{ann}_R(m_i))$; we are using finiteness here. Also, observe that $\mathrm{Supp}(M) = \bigcup_i \mathrm{Supp}(Rm_i)$: the containment $\supseteq$ is clear since $(Rm_i)_{\mathfrak{p}} \subseteq M_{\mathfrak{p}}$, while $\subseteq$ follows from the fact that the images of m_i's in $M_{\mathfrak{p}}$ generate $M_{\mathfrak{p}}$ for each $\mathfrak{p}$. Thus, we reduce to the case of Rm_i, and this follows from fact that $m_i/1 = 0$ in $M_{\mathfrak{p}}$ if and only if $(R \smallsetminus \mathfrak{p}) \cap \mathrm{ann}_R(m_i) \neq \varnothing$, which happens if and only if $\mathrm{ann}_R(m_i) \not\subseteq \mathfrak{p}$. □

The finite generating hypothesis is necessary!

Example 4.9. Let K be a field, and $R = K[x]$. Take $M = R_x/R = \bigoplus_{i>0} Kx^{-i}$. 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, $\mathrm{Supp}(M) = \{(x)\}$. Indeed, any element of M is killed by a large power of x, so $W^{-1}M = 0$ if $x \in W$, so $\mathrm{Supp}(M) \subseteq \{(x)\}$.

On the other hand, the annihilator of the class of x^{-n} is x^n, so $\mathrm{ann}_R(M) \subseteq \bigcap_{n \in \mathbb{N}} (x^n) = 0$.

Example 4.10. Let $R = \mathbb{C}[x]$, and $M = \bigoplus_{n \in \mathbb{Z}} R/(x-n)$.

On the one hand, $\mathrm{Supp}(M) = \{(x-n) \mid n \in \mathbb{Z}\}$. Indeed, $M_{\mathfrak{p}} = \bigoplus_{n \in \mathbb{Z}} (R/(x-n))_{\mathfrak{p}}$, 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 the support is not even closed.

Proposition 4.11. *Let R be a ring, L, M, N be modules, and $m \in M$.*

1. *$m = 0 \Leftrightarrow m/1 = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec} R \Leftrightarrow m/1 = 0$ in $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \in \operatorname{Max} R$.*
2. *If $0 \to L \to M \to N \to 0$ is exact, then $\operatorname{Supp}(L) \cup \operatorname{Supp}(N) = \operatorname{Supp}(M)$.*
3. *$M = 0 \Leftrightarrow M_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R \Leftrightarrow M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \in \operatorname{Max} R$.*

Proof. 1. The implications $\Rightarrow$ are clear. To show the last implies the first, we show the comtrapositive. If $m \neq 0$, its annihilator is a proper ideal, which is contained in a maximal ideal, so $V(\operatorname{ann}_R m) = \operatorname{Supp}(Rm)$ contains a maximal ideal.

2. For any $\mathfrak{p}$, we have $0 \to L_{\mathfrak{p}} \to M_{\mathfrak{p}} \to N_{\mathfrak{p}} \to 0$ is exact. If $\mathfrak{p} \in \operatorname{Supp}(L) \cup \operatorname{Supp}(N)$, then $L_{\mathfrak{p}}$ or $N_{\mathfrak{p}}$ is nonzero, so $M_{\mathfrak{p}}$ must be. On the other hand, if $\mathfrak{p} \notin \operatorname{Supp}(L) \cup \operatorname{Supp}(N)$, then $L_{\mathfrak{p}} = N_{\mathfrak{p}} = 0$, so $M_{\mathfrak{p}} = 0$.

3. The implications $\Rightarrow$ are clear. To show the last implies the first, we show the comtrapositive. If $m \neq 0$, consider $Rm \subseteq M$. By part (1), there is a maximal ideal in $\operatorname{Supp}(Rm)$, and by part (2), this maximal ideal is in $\operatorname{Supp}(M)$ as well. □

4.2 Associated primes and prime filtrations

We now refine our decomposition of ideals/modules.

Definition 4.12. *Let R be a ring, and M a module. We say that $\mathfrak{p} \in \operatorname{Spec}(R)$ is an* associated prime *of M if $\mathfrak{p} = \operatorname{ann}_R(m)$ for some $m \in M$. Equivalently, $\mathfrak{p}$ is associated to M if there is an injective homomorphism $R/\mathfrak{p} \hookrightarrow M$. We write $\operatorname{Ass}_R(M)$ 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; but we'll try to write $\operatorname{Ass}_R(R/I)$.*

Lemma 4.13. *If $\mathfrak{p}$ is prime, $\operatorname{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.*

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 ideals. □

Lemma 4.14. *If R is Noetherian, and M an arbitrary R-module, then*

1. *$\operatorname{Ass}(M) = \varnothing \Leftrightarrow M = 0$, and*
2. *$\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p} = \{$zerodivisors on $M\} := \{r \in R \mid rm = 0$ for some $m \in M \setminus \{0\}\}$.*

Additionally, if R and M are ($\mathbb{Z}$-)graded and $M \neq 0$, M has an associated prime that is homogeneous.

Proof. ($\Leftarrow$) is clear in part 1 (and certainly doesn't require Noetherian).

The interesting direction of 1 and part 2 will both follow from the fact that any ideal of the form $\operatorname{ann}_R(m)$ is contained in an associated prime; such a prime will certainly exist, and if something is a zerodivisor, it must belong to an associated prime.

Any element in the (nonempty) set $\{\operatorname{ann}_R(m) \mid m \in M \setminus 0\}$ is contained in a maximal element, by Noetherianity. Let $I = \operatorname{ann}(m)$ be such an element, and let $rs \in I$, $s \notin I$. Clearly $\operatorname{ann}(sm) \supseteq \operatorname{ann}(m)$, and equality holds by maximality. Then, $(rs)m = r(sm) = 0$, so $r \in \operatorname{ann}(sm) = \operatorname{ann}(m) = I$. Thus, I is prime.

For the graded case, replace the set about with the annihilators of homogeneous elements. Such annihilator is homogeneous, since if m is homogeneous, and $fm = 0$, 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.

The same argument above works if we take $\{\operatorname{ann}_R(m) \mid m \in M \smallsetminus 0 \text{ homogeneous }\}$, using the following lemma. □

Lemma 4.15. *If R is $\mathbb{Z}$-graded, an ideal with the property*

$$\forall r, s \in R \text{ homogeneous} \quad rs \in I \Rightarrow r \in I \text{ or } s \in I$$

is prime.

Proof. We need to show that this property implies that $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$. We induce on the number of nonzero homogeneous components of a plus the number of nonzero homogeneous components of b. The base case is when this is two, coming directly from the hypotheses. Otherwise, write $a = a' + a_m$, $b = b' + b_n$, where a_m, b_n are the largest homogeneous components of a, b respectively. We have $ab = (a'b' + a_mb' + b_na') + a_mb_n$, where a_mb_n is either the largest homogeneous component of ab or else it is zero. Either way, $a_mb_n \in I$, so $a_m \in I$ or $b_n \in I$; WLOG $a_m \in I$. Then $ab = a'b + a_mb$, and $ab, a_mb \in I$, so $a'b \in I$, and the total number of homogeneous pieces is smaller, so by induction, either $a' \in I$ so that $a \in I$, or else $b \in I$. □

Lemma 4.16. *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 $R/\mathfrak{p} \hookrightarrow N$. □

24 Septiembre

We will need a bit of notation for graded modules to help with the next statement.

Definition 4.17. *Let R and M be T-graded, and $t \in T$. The* shift *of M by t is the graded R-module $M(t)$ with graded pieces $M(t)_i := M_{t+i}$. This is isomorphic to M as an R-module without the grading.*

Theorem 4.18. *If R is a Noetherian ring, and M is a finitely generated module, then there exists a* filtration *of M*

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

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.*

If additionally R and M are $\mathbb{Z}$-graded, there is a filtration as above 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.

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.

In the graded case, if $\mathfrak{p}_i$ is the annihilator of an element m_i of degree t_i, we have a degree-preserving map $(R/\mathfrak{p}_i)(t_i) \cong Rm_i$ sending the class of 1 to m_i. The rest of the proof is the same. □

Prime filtrations often allow us to reduce statements about finitely generated modules to statements about quotient domains of R: modules of the form $R/\mathfrak{p}$ for primes $\mathfrak{p}$.

Corollary 4.19. *If R is a Noetherian ring, and M is a finitely generated module, and*

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

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.*
- *If M is graded, $\operatorname{Ass}_R(M)$ is a finite set of homogeneous primes.*

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 consequences follow from the previous theorem. □

Example 4.20. Any subset $X \subseteq \operatorname{Spec}(R)$ (for any R) can be realized as $\operatorname{Ass}(M)$ for some M: take $M = \bigoplus_{\mathfrak{p} \in X} R/\mathfrak{p}$. Of course, if X is infinite, M is not finitely generated.

Example 4.21. 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 $m \leq n$. 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 $x^{1/2-m/2n}$.

We will need that associated primes localize.

Theorem 4.22 (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

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

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 $\mathfrak{p} \in \operatorname{Ass}_R(M)$. □

Corollary 4.23. *Let R be Noetherian, and M be an R-module.*

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

2. *If M is finitely generated, then* $\operatorname{Min}(\operatorname{ann}_R(M)) \subseteq \operatorname{Ass}_R(I)$. *In particular,* $\operatorname{Min}(I) \subseteq \operatorname{Ass}_R(R/I)$.

Proof. 1. ($\supseteq$): Let $\mathfrak{p} \in \operatorname{Ass}_R(M)$ and let $\mathfrak{p} = \operatorname{ann}_R(m)$ for $m \in M$. Let $\mathfrak{q} \in V(\mathfrak{p})$. We have $0 \to R/\mathfrak{p} \xrightarrow{m} M$ exact, and thus $0 \to (R/\mathfrak{p})_\mathfrak{q} \to M_\mathfrak{q}$ is exact, with $(R/\mathfrak{p})_\mathfrak{q}$ nonzero, so $M_\mathfrak{q} \neq 0$.

($\subseteq$): Suppose that $\mathfrak{q}$ is not in the right-hand side in the equation above, so that $\mathfrak{q}$ does not contain any associated prime of M. Then there is no associated prime of M that does not intersect $R \smallsetminus \mathfrak{q}$, so $\operatorname{Ass}_{R_\mathfrak{q}}(M_\mathfrak{q}) = \varnothing$, so $M_\mathfrak{q} = 0$.

2. We have that $V(\operatorname{ann}_R(M)) = \operatorname{Supp}_R(M) = \bigcup_{\mathfrak{p}\in \operatorname{Ass}_R(M)} V(\mathfrak{p})$, so the minimal elements of both sets agree. In particular, the right hand side has the minimal primes of $\operatorname{ann}_R(M)$ as minimal elements, and they must be associated primes of M, or else this would contradict minimality.

□

Definition 4.24. *If I is an ideal, then an associated prime of I that is not a minimal prime of I is called an* embedded prime *of I.*

25 Septiembre

We take a quick detour to introduce an important lemma.

Lemma 4.25 (Prime avoidance)**.** *Let R be a ring, $I_1, \dots, I_n, J$ be ideals, and suppose that I_i is prime for $i > 2$ (at most two are not prime).*

If $J \not\subseteq I_i$ for all i, then $J \not\subseteq \bigcup_i I_i$; 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 $J \not\subseteq I_i$ 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 $a_1, \dots, a_{n-1} \in I_n$, a contradiction.

If all I_i are homogeneous and prime, we proceed as above, replacing a_n and $a_1, \dots, a_{n-1}$ 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 4.26. *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 $I \subseteq \bigcup_{\mathfrak{p}\in \operatorname{Ass}(M)}(\mathfrak{p})$. By the assumptions, this is a finite set of primes. By prime avoidance, $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M)$. That is $I \subseteq \operatorname{ann}_R(m)$ for some $m \in M$. □

4.3 Primary decomposition

We refine our decomposition theory once again.

Definition 4.27. *We say that an ideal is* primary *if $xy \in I \Rightarrow x \in I$ or $y \in \sqrt{I}$. We say that an ideal is* $\mathfrak{p}$-primary *if I is primary and $\sqrt{I} = \mathfrak{p}$.*

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

Example 4.28.

1. If R is a UFD, 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 $xy \in (f^n) \Leftrightarrow f^n | xy \Leftrightarrow f^n | x$ or $f | y \Leftrightarrow x \in (f^n)$ 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 $h \notin \sqrt{(a)}$.
2. In $R = \mathbb{C}[x, y, z]$, 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 has a term of degree zero or one, so is not in I.
3. In $R = \mathbb{C}[x, y, z]$, 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 4.29. *If R is Noetherian, the following are equivalent:*

1. *$\mathfrak{q}$ is primary.*
2. *Every zerodivisor in $R/\mathfrak{q}$ is nilpotent.*
3. *$\mathrm{Ass}(R/\mathfrak{q})$ is a singleton.*
4. *$\mathfrak{q}$ has one minimal prime, and no embedded primes.*
5. *$\sqrt{\mathfrak{q}} = \mathfrak{p}$ is prime and $r \in R$, $w \in R \setminus \mathfrak{p}$, $rw \in \mathfrak{q}$ implies $r \in \mathfrak{q}$.*
6. *$\sqrt{\mathfrak{q}} = \mathfrak{p}$ is prime, and $\mathfrak{q}R_{\mathfrak{p}} \cap R = \mathfrak{q}$.*

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 $\mathfrak{q}$.

(2) $\iff$ (3): (2) translates to $\bigcup_{\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(R/\mathfrak{q})} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{q})} \mathfrak{p}$. This holds if and only if there is one associated prime.

(3) $\iff$ (4): is clear.

(1) $\iff$ (5): Given the observation about that the radical of a primary ideal is prime, this is just a rewording of the definition.

(5) $\iff$ (6): We already know this from the discussion on behavior of ideals in localizations. □

Remark 4.30. Let I be an ideal with $\sqrt{I} = \mathfrak{m}$ a maximal ideal. If R is Noetherian, then $\mathrm{Ass}_R(R/I)$ is nonempty and contained in $\mathrm{Supp}(R/I) = V(I) = \{\mathfrak{m}\}$, so must be $\mathfrak{m}$, and hence I is primary. Note that the assumption that $\mathfrak{m}$ is maximal was necessary here.

Next, we observe:

Lemma 4.31. *If $I_1, \dots, I_t$ are ideals, then $\operatorname{Ass}(R/(\bigcap_{j=1}^t I_j)) \subseteq \bigcup_{j=i}^t \operatorname{Ass}(R/I_j)$. In particular, a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

Proof. There is an injection $R/(I_1 \cap I_2) \hookrightarrow R/I_1 \oplus R/I_2$. 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 obvious induction.

The latter statement follows from characterization #3 above. □

Definition 4.32 (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 4.33. By the previous lemma, we can turn a primary decomposition into a minimal one by combining the terms with the same radical, then removing redundant terms.

Theorem 4.34 (Existence of primary decompositions)**.** *If R is Noetherian, then every ideal of R admits a primary decomposition.*

Proof. We will say that an ideal is irreducible if it cannot be written as a proper intersection of larger ideals. If R is Noetherian, any ideal of R can be expressed as a finite intersection of irreducible ideals: if not, there would be an ideal maximal with the property of not being an intersection of irreducible ideals, which must be an intersection of two larger ideals, each of which are finite intersections of irreducibles, giving a contradiction.

Now, we claim that every irreducible ideal is primary. To establish the contrapositive, take $xy \in \mathfrak{q}$ with $x \notin \mathfrak{q}$, $y \notin \sqrt{\mathfrak{q}}$. The ascending chain of ideals $J_n = (\mathfrak{q} : y^n)$ stabilizes for some n; this means that $y^{n+1} f \in \mathfrak{q} \;\Rightarrow\; y^n f \in \mathfrak{q}$. We will show that $(\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x)) = \mathfrak{q}$.

The containment $\mathfrak{q} \subseteq (\mathfrak{q} + (y^n)) \cap (\mathfrak{q} + (x))$ is clear. If a is in the RHS, we have $a = q + by^n$ for some $q \in \mathfrak{q}$, and $ya \in \mathfrak{q}$ (since $a \in \mathfrak{q} + (x)$), so $by^{n+1} \in \mathfrak{q}$. Then, $by^n \in \mathfrak{q}$ by the hypothesis on the chain J_n, and hence $a \in \mathfrak{q}$, as required. This shows that $\mathfrak{q}$ is decomposable, concluding the proof. □

There are also some uniqueness theorems for primary decomposition.

1 Octubre

Theorem 4.35 (First uniqueness theorem for primary decompositions)**.** *If I is an ideal in a Noetherian ring R, then for any minimal primary decomposition of I, $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, we have $\{\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_t}\} = \operatorname{Ass}(R/I)$. 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 above. We just need to show that in a minimal decomposition as above, every $\mathfrak{p}_j := \sqrt{\mathfrak{q}_j}$ is an associated prime.

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 has an associated prime $\mathfrak{a}$; let $\mathfrak{a}$ be the annihilator of $\overline{x_j}$ in I_j/I, with $x_j \in R$. Since $\mathfrak{q}_j x_j \subseteq I$, we have that $\mathfrak{q}_j$ is contained in the annihilator of $\overline{x_j}$, and since $\mathfrak{p}_j$ is the unique minimal prime of $\mathfrak{q}_j$ (and $\mathfrak{a}$ is a prime containing $\mathfrak{q}_j$), $\mathfrak{p}_j \subseteq \mathfrak{a}$. 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 $r \in \mathfrak{p}_j$ by the definition of primary. Thus, $\mathfrak{a} \subseteq \mathfrak{p}_j$, so $\mathfrak{a} = \mathfrak{p}_j$. □

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

Proof. We observe that a localization $\mathfrak{q}_{\mathfrak{a}}$ of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is either the unit ideal (if $\mathfrak{a} \not\subseteq \mathfrak{p}$), or is a $\mathfrak{p}_{\mathfrak{a}}$-primary ideal: this follows from the fact that the associated primes of $R/\mathfrak{q}$ localize.

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

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

is a (not necessarily minimal) primary decomposition. In a minimal decomposition, choose a minimal prime $\mathfrak{a} = \mathfrak{p}_i$ to get $I_{\mathfrak{p}_i} = (\mathfrak{q}_i)_{\mathfrak{p}_i}$; the other components in the intersection become the unit ideal since their radicals are not contained in $\mathfrak{p}_i$. 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. □

Example 4.37. If R is Noetherian, and I is a radical ideal, we have that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$, where $\mathfrak{p}_i$ are the minimal primes of I. This is the only primary decomposition of a radical ideal.

Example 4.38. 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.

Definition 4.39 (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 4.40. *Let R be Noetherian, and $\mathfrak{p}$ a prime ideal of R.*

1. $\mathfrak{p}^{(n)} = \{r \in R \mid \exists s \notin \mathfrak{p} : rs \in \mathfrak{p}^n\}$.
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 a characterization of primary above. 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 above. □

Example 4.41. 1. In $R = K[x, y, z]$, $\mathfrak{p} = (y, z)$, we have $\mathfrak{p}^{(n)} = \mathfrak{p}^n$ for all n. This follows along the same lines as an example above.

2. In $R = K[x, y, z] = (xy - z^2)$, $\mathfrak{p} = (y, z)$, we have $\mathfrak{p}^{(2)} \neq \mathfrak{p}^2$. Indeed, $xy = z^2 \in \mathfrak{p}^2$, and $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}^{(2)} \setminus \mathfrak{p}^2$.

3. Let $X = X_{3\times 3}$ be a 3×3 matrix of indeterminates, and $K[X]$ be a polynomial ring over a field K. Let $\mathfrak{p} = I_2(X)$ be the ideal generated by 2×2 minors of X. We will write $\Delta_{\substack{i|k\\j|l}}$ for the determinant of the submatrix with rows i, j and columns k, l. We find

$$\begin{aligned} x_{11}\det(X) &= x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}} \\ &= (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{11}x_{32}\Delta_{\substack{1|1\\2|3}} + x_{11}x_{33}\Delta_{\substack{1|1\\2|2}}) - (x_{11}x_{31}\Delta_{\substack{1|2\\2|3}} - x_{12}x_{31}\Delta_{\substack{1|1\\2|3}} + x_{13}x_{31}\Delta_{\substack{1|1\\2|2}}) \\ &= -\Delta_{\substack{1|1\\3|2}}\Delta_{\substack{1|1\\2|3}} + \Delta_{\substack{1|1\\3|3}}\Delta_{\substack{1|1\\2|2}} \in I_2(X)^2. \end{aligned}$$

Note that in the second row, we subtracted the Laplace expansion of determinant of the matrix with row 3 replaced by another copy of row 1. That is, we subtracted zero.

Chapter 5

Spec and dimension

5.1 Dimension and height

Definition 5.1.

- *A* chain of primes *of* length n *in a ring* R *is*
$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n \quad \textit{with } \mathfrak{a}_i \in \operatorname{Spec}(R).$$
- *A chain of primes as above is* saturated *if for each* i*, there is no* $\mathfrak{q} \in \operatorname{Spec}(R)$ *with* $\mathfrak{a}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{a}_{i+1}$.
- *The* dimension *or* Krull dimension *of a ring* R *is the supremum of the lengths of chains of primes in* R*. Equivalently, it is the supremum of the lengths of saturated chains of primes in* R*.*
- *The* height *of a prime* $\mathfrak{p}$ *is the supremum of the lengths of chains of primes in* R *that end in* $\mathfrak{p}$ *(i.e.,* $\mathfrak{p} = \mathfrak{a}_n$ *above). Equivalently, it is the supremum of the lengths of saturated chains of primes in* R *that end in* $\mathfrak{p}$*.*
- *The* height *of an ideal* I *is the infimum of the heights of the minimal primes of* I*.*

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

Remark 5.2.

1. If $\mathfrak{p}$ is prime, then $\dim(R/\mathfrak{p})$ is the supremum of the lengths of (saturated) chains of primes in R
$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n$$
with each $\mathfrak{a}_i \in V(\mathfrak{p})$.
2. If I is an ideal, then $\dim(R/I)$ is the supremum of the lengths of (saturated) chains of primes in R
$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n$$
with each $\mathfrak{a}_i \in V(I)$.
3. If W is a multiplicative set, then $\dim(W^{-1}R) \leq \dim(R)$.
4. If $\mathfrak{p}$ is prime, then $\operatorname{height}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$.
5. If $\mathfrak{q} \supseteq \mathfrak{p}$ 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
$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n$$
with $\mathfrak{a}_0 = \mathfrak{p}$ and $\mathfrak{a}_n = \mathfrak{q}$.

6. $\dim(R) = \sup\{\text{height}(\mathfrak{m}) \mid \mathfrak{m} \in \text{Max}(R)\}$.
7. $\dim(R) = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \text{Min}(R)\}$.
8. If $\mathfrak{p}$ is prime, $\dim(R/\mathfrak{p}) + \text{height}(\mathfrak{p}) \leq \dim(R)$.
9. If I is an ideal, $\dim(R/I) + \text{height}(I) \leq \dim(R)$.
10. A prime has height zero if and only if it is a minimal prime.

3 Octubre

We will need a few theorems before we can compute many examples, but we can handle a few basic cases.

Example 5.3. 1. The dimension of a field is zero.

2. A ring is zero-dimensional if and only if every minimal prime 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, a principal ideal domain has dimension one.
4. If R is a UFD, I is a prime of height one if and only if $I = (f)$ for a prime element f.

   To see this, note that if $I = (f)$ with f irreducible, and $0 \subsetneqq \mathfrak{p} \subseteq I$, then $\mathfrak{p}$ contains some nonzero multiple of f, say af^n with a and f coprime. Since $a \notin I$, $a \notin \mathfrak{p}$, so we must have $f \in \mathfrak{p}$, so $\mathfrak{p} = (f)$. Thus, I has height one. On the other hand, if I is a prime of height one, we claim I contains an irreducible element. Indeed, I is nonzero, so contains some $f \neq 0$, and primeness implies one of the prime factors of f is contained in I. Thus, any nonzero prime contains a prime ideal of the form (f), so a height one prime must be of this form.
5. It follows from the definition that if K is a field, then $\dim(K[x_1, \ldots, x_d]) \geq d$, since there is a saturated chain of primes $(0) \subsetneqq (x_1) \subsetneqq (x_1, x_2) \subsetneqq \cdots \subsetneqq (x_1, \ldots, x_d)$.

We pose a related definition for modules.

Definition 5.4. *The* dimension *of an R-module M is defined as* $\dim(R/\operatorname{ann}_R(M))$.

Note that if M is finitely generated, $\dim(M)$ is the same as the largest length of a chain of primes in $\text{Supp}_R(M)$.

Definition 5.5.
- *A ring is **catenary** if for every pair of primes $\mathfrak{q} \supseteq \mathfrak{p}$ in R, every saturated chain of primes*
$$\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots \subsetneqq \mathfrak{a}_n$$
with $\mathfrak{a}_0 = \mathfrak{p}$ and $\mathfrak{a}_n = \mathfrak{q}$ 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.*

Example 5.6. $\dfrac{K[x,y,z]}{(xy, xz)}$ is not equidimensional: note first that $\text{Min}(R) = \{(x), (y,z)\}$. We can see this by computing $\text{Min}((xy, xz))$ in $K[x,y,z]$: (x) and (y,z) are prime, and $(x) \cap (y,z) = (xy, xz)$, verifying the claim. Now, the height of $(x-1, y, z)$ is one: it contains the minimal prime (y,z), and any saturated chain from (y,z) to $(x-1,y,z)$ corresponds to a saturated chain from (0) to $(x-1)$ in $K[x]$, which must have length one since this is a PID. The height of $(x, y-1, z)$ is at least two, as witnessed by the chain $(x) \subseteq (x, y-1) \subseteq (x, y-1, z)$.

Example 5.7. $\mathbb{Z}_{(2)}[x]$ is a domain that is not equidimensional: consider the maximal ideal $(2, x)$ that has height at least two, and the maximal ideal $(2x - 1)$; this is maximal since the quotient is $\mathbb{Q}$!

Remark 5.8.
1. If $\dim(R) < \infty$, R is a domain, and $f \neq 0$, then $\dim(R/(f)) < \dim(R)$.
2. If R is equidimensional, then $\dim(R/(f)) < \dim(R)$ if and only if $f \notin \bigcup_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p}$.
3. In general, $\dim(R/(f)) < \dim(R)$ if and only if $f \notin \bigcup_{\substack{\mathfrak{p} \in \operatorname{Min}(R) \\ \dim(R/\mathfrak{p}) = \dim(R)}} \mathfrak{p}$.
4. $f \notin \bigcup_{\mathfrak{p} \in \operatorname{Min}(R)} \mathfrak{p}$ if and only if $\dim(R/(\mathfrak{p} + (f))) < \dim(R/\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Min}(R)$.

The one warning to make about dimension before we get too optimistic is that there are Noetherian rings of infinite dimension.

Example 5.9. Let $R = K[x_1, x_2, \dots]$. R is clearly infinite-dimensional, but is Noetherian. Let

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

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

5.2 Over, up, down theorems

In this section, we will collect theorems of three forms about the spectrum of a ring: theorems that assert that the map on Spec is surjective, and theorems about lifting chains of primes.

Recall that the fiber ring over $\mathfrak{p}$ of a homomorphism $\varphi : R \to S$ is given by

$$\kappa_\varphi(\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S),$$

and that

$$\operatorname{Spec}(\kappa_\varphi(\mathfrak{p})) \cong (\varphi^*)^{-1}(\mathfrak{p}),$$

the subspace of $\operatorname{Spec}(S)$ consisting of primes that contract to $\mathfrak{p}$. As a special case, we write $\kappa(\mathfrak{p})$ for the fiber of the identity map; this is $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$, the residue field of the local ring $R_\mathfrak{p}$.

Lemma 5.10 (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 5.11. 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 $x^n R$ is prime, while $x^n S$ is not radical.

Corollary 5.12. *If $R \subseteq S$ is a direct summand, then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is surjective.*

Proof. From the homework, 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 5.13. *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.

Exercise 5.14. 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 5.15 (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. □

Theorem 5.16 (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 5.17. 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 5.18 (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 $R/\mathfrak{p} \hookrightarrow S/\mathfrak{p}S$ (injective by the lemma above) is integral; take an integral equation for a representative. Furthermore, localizing at $(R \setminus \mathfrak{p})$ preserves integrality: if $x \in S$ and $w \in R \setminus \mathfrak{p}$, 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 $\mathfrak{p}$. □

8 Octubre

Corollary 5.19. *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 $\mathfrak{p}$. If, moverover, $S = \sum_{i=1}^t Rs_i$ is generated as a module by t elements, then for any prime of R, at most t primes of S map 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.

for the second statement, we have $\kappa_\phi(\mathfrak{p}) = \sum_{i=1}^t \kappa(\mathfrak{p})\bar{s_i}/1$, and hence $\kappa_\phi(\mathfrak{p})$ is a zero-dimensional ring that is a $\kappa(\mathfrak{p})$-vector space of dimension at most t. We have a minimal primary decomposition $(0)_{\kappa_\phi(\mathfrak{p})} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ where $\sqrt{\mathfrak{q}_i}$ are distinct maximal ideals; these maximal ideals are in bijection with the primes mapping to $\mathfrak{p}$ in S. Thus, for $i \neq j$, $V(\mathfrak{q}_i + \mathfrak{q}_j) = V(\mathfrak{q}_i) \cap V(\mathfrak{q}_j) = \varnothing$, so $\mathfrak{q}_i + \mathfrak{q}_j = \kappa_\phi(\mathfrak{p})$, and by the Chinese Remainder Theorem, $\kappa_\phi(\mathfrak{p}) \cong \kappa_\phi(\mathfrak{p})/\mathfrak{q}_1 \times \cdots \times \kappa_\phi(\mathfrak{p})/\mathfrak{q}_s$. The map $\kappa(\mathfrak{p}) \to \kappa_\phi(\mathfrak{p})/\mathfrak{q}_i$ is nonzero for each i (since it is integral), so each factor is a $\kappa(\mathfrak{p})$-vector space. Considering vector space dimension, find that the number of factors s is at most t. □

Corollary 5.20. *If $R \to S$ is integral, then* $\operatorname{height}(\mathfrak{q}) \leq \operatorname{height}(\mathfrak{q} \cap R)$ *for any $\mathfrak{q} \in \operatorname{Spec}(S)$. In particular,* $\dim(S) \leq \dim(R)$.

Proof. Given a chain of primes $\mathfrak{a}_0 \subsetneq \cdots \subsetneq \mathfrak{a}_n = \mathfrak{q}$ 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 5.21 (Going up)**.** *If $R \to S$ 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 $\mathfrak{q}' \cap R = \mathfrak{p}'$.*

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 5.22. *If $R \subseteq S$ is integral, then* $\dim(R) = \dim(S)$.

Proof. We just need to show that $\dim(R) \leq \dim(S)$. Given a chain of primes $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ 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 $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ with $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Continuing, we can build a chain of distinct primes in S of length n. □

Definition 5.23. *A domain is* normal *if it is integrally closed in its field of fractions.*

Lemma 5.24. *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 5.25. *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 $x_1 = x, x_2, \ldots, x_u$ be the roots of f. Since $f(t)$ divides a monic equation for x, each x_i is integral over R.

Let $S = R[x_1, \ldots, x_u] \subseteq \overline{K}$. 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 5.26 (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 $W = (S \setminus \mathfrak{q})(R \setminus \mathfrak{p}')$ be the multiplicative set consisting of products of elements in $S \setminus \mathfrak{q}$ and $R \setminus \mathfrak{p}'$. 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 $W^{-1}(S/\mathfrak{p}'S) = (S \setminus \mathfrak{q})^{-1}\kappa_S(\mathfrak{p}')$ 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 $r \in R \setminus \mathfrak{p}', s \in S \setminus \mathfrak{q}$, 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. □

Remark 5.27. We have used the fact that our rings are domains to put the theory of minimal polynomials to use. The one hypothesis we can weaken is that the target is a domain: it suffices to assume that it is torisonfree as a module over the source. Here's why we can't get rind of more hypotheses.

Let $R = K[x] \subseteq S = K[x,y]/(xy, y^2 - y)$. R is a normal domain, and the inclusion is integral: $y^2 - y = 0$ is an integral dependence relation for y over R, so S is generated by one integral element. Now, $(1-y)$ is a minimal prime of S: $y \in S \smallsetminus (1-y)$, so x goes to zero in the localization (since $xy = 0$) and $1 - y$ goes to zero in the localization (since $y(1-y) = 0$), so the localization is a copy of K, which has only one prime, (0). We have $x = x - xy = x(1-y) \in (1-y)$, so the contraction contains (x), so must be (x). But, by minimality, we can't "go down" from $(1-y)$ to a prime lying over (0).

The normality hypothesis is important too. Take $R = K[x(1-x), x^2(1-x), y, xy] \subseteq S = K[x,y]$. The element x is integral over R: $x(1-x) \in R$ is a recipe: x is a root of $z^2 - z - x(1-x)$. Note that x is in the fraction field of R, so this element shows both that S is integral over R, and that R is not normal. Now, $\mathfrak{q} = (1-x, y) \subseteq S$ is a maximal ideal lying over the maximal ideal $\mathfrak{p}$ generated by the specified generating set in R. We have $xS \cap R = (x(1-x), x^2(1-x), xy)R = \mathfrak{p}'$, but we claim that no prime contained in $\mathfrak{q}$ lies over $\mathfrak{p}'$. Such a prime must contain $x(1-x)$ and xy, but not x (this would make it the unit ideal), so must contain y and $1-x$, and the contraction is then $\mathfrak{p}$, which is too big!

Corollary 5.28. *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 $\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{q} \cap R)$. 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 $\mathfrak{q}$. □

10 Octubre

5.3 Noether normalization and dimension of affine rings

Lemma 5.29 (Making a pure-power leading term)**.** *1. Let A be a domain, and $f \in R = A[x_1, \ldots, x_n]$ 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 $A[x_1, \ldots, x_{n-1}]$, has leading term dx_n^a for some $d \in A$, $a \in \mathbb{N}$.*

2. Let K be an infinite field, and $f \in R = K[x_1, \ldots, x_n]$, 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 $K[x_1, \ldots, x_{n-1}]$, has leading term kx_n^N for some (nonzero) $k \in K$.

Proof. 1. The map ϕ sends a monomial term $dx_1^{a_1} \cdots x_n^{a_n}$ to a polynomial with unique highest degree term $dx_n^{a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1} N + a_n}$. Since each a_i is less than N in each monomial, the map $(a_1, \ldots, a_n) \mapsto a_1 N^{n-1} + a_2 N^{n-2} + \cdots + a_{n-1} N + a_n$ is injective when restricted to the set of exponent tuples; thus, none of the terms can cancel. We find that the leading term is of the promised form.

2. We just need to show that the x^N coefficient is nonzero for some choice of a's. You can check that the coefficient of the x^N term is $f(-a_1, \ldots, -a_{n-1}, 1)$. But if this, thought of as a polynomial in the a's, is identically zero, then f must be the zero polynomial. □

Theorem 5.30 (Noether Normalization)**.** *1. 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 $K[x_1, \ldots, x_t]$.*

2. Let K be an infinite field, and R be a finitely generated $\mathbb{N}$-graded K-algebra with $R_0 = K$ and $R = K[R_1]$. Then there are homogeneous elements $x_1, \ldots, x_t \in R_1$ algebraically independent over K such that 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.

In the graded case, we use the graded part of the previous lemma. □

Remark 5.31. There also exist Noether normalizations for quotients of power series rings over fields: after a change of coordinates, one can rewrite any nonzero power series in $K[\![x_1, \ldots, x_n]\!]$ as a series of the form $u(x_n^d + a_{d-1}x_n^{d-1} + \cdots + a_0)$ for a unit u and $a_0, \ldots, a_{d-1} \in K[\![x_1, \ldots, x_{n-1}]\!]$. This is called *Weierstrass preparation*. The proof of the Noether normalization theorem proceeds in essentially the same way. Thus, given $K[\![x_1, \ldots, x_n]\!]/I$, we have some module-finite inclusion of another power series ring $K[\![z_1, \ldots, z_d]\!] \subseteq K[\![x_1, \ldots, x_n]\!]/I$.

Theorem 5.32. *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.*

The same holds in a quotient of a power series ring over a field.

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

$$0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_k = \mathfrak{m}$$

and consider the contractions to $A = K[z_1, \ldots, z_d]$:

$$0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_k.$$

By the saturated condition, $\mathfrak{q}_1$ has height 1, and so does $\mathfrak{p}_1$, by going down. 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,

$$0 = \mathfrak{q}_1/\mathfrak{q}_1 \subsetneqq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_k/\mathfrak{q}_1 = \mathfrak{m}/\mathfrak{q}_1$$

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 $k = d$.

The same proof holds for quotients of power series rings. □

Corollary 5.33. *The dimension of the polynomial ring $K[x_1, \ldots, x_d]$ is d.*

Corollary 5.34. *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 $R = K[f_1, \ldots, f_s] \cong K[x_1, \ldots, x_s]/I$ for some ideal I. We have $\dim(R) \leq s$, for certain. If $I \neq 0$, then $\dim(R) < s$, since the zero ideal is not contained in I. □

Corollary 5.35. *Let R be a finitely generated algebra oor a quotient of a power series ring over a field.*

- *R is catenary.*

If additionally R is a domain, then

- *R is equidimensional, and*
- *$\mathrm{ht}(I) = \dim(R) - \dim(R/I)$ 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 $\mathrm{ht}(I) = \min\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$ and $\dim(R/I) = \max\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Min}(I)\}$. 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 $\mathrm{ht}(\mathfrak{p})$ 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. □

Corollary 5.36. *If R is a finitely generated domain over a field K, then* $\dim(R) = \mathrm{trdeg}_K(\mathrm{frac}(R))$.

Proof. If $R \subseteq S$ is module-finite, then $\text{frac}(R) \subseteq \text{frac}(S)$ is algebraic, and hence they have the same transcendence degree over K. In particular, if $A = K[z_1, \ldots, z_d]$ is a Noether normalization for R,

$$\text{trdeg}_K(\text{frac}(R)) = \text{trdeg}_K(\text{frac}(A)) = \text{trdeg}_K(K(z_1, \ldots, z_d)) = d = \dim(A) = \dim(R). \qquad \square$$

15 Octubre

Example 5.37. We want to try out our dimension theorems to give a few different proofs that $R = \dfrac{K[x,y,z]}{(y^2 - xz)}$ has dimension two, for a field K.

First: $K[x,z]$ is a Noether normalization for R, so the dimension is 2.

Second: we observe that $y^2 - xz$ is irreducible, e.g., by thinking of it as a polynomial in y and applying Eisenstein's criterion. Then $(y^2 - xz)$ is a prime of height one, so the dimension of R is $\dim(K[x,y,z]) - \text{height}((y^2 - xz)) = 3 - 1 = 2$.

Third: we want the use the characterization by transcendence dimension. To do this, we will show that $R \cong K[u^2, uv, v^2] \subseteq K[u,v]$. Let $S = K[x,y,z]$, and consider the surjective K-algebra homomorphism $\phi : S \to K[u^2, uv, v^2]$ given by $\phi(x) = u^2, \phi(y) = uv, \phi(z) = v^2$. Clearly, $(y^2 - xz) \subseteq \ker(\phi)$; we claim this is an equality. To show this claim, first assume that $K = \overline{K}$. We have $Z_K(\ker(\phi)) \subseteq Z_K((y^2 - xz))$. Let $(a,b,c) \in Z_K((y^2 - xz))$. Let $\alpha, \gamma \in K$ be such that $\alpha^2 = a, \gamma^2 = c$; we can do this since K is algebraically closed. Then $b^2 = ac = (\alpha\gamma)^2$. Replacing γ with $-\gamma$ if necessary, we can assume that in fact $b = \alpha\gamma$. Then $(a,b,c) = (\alpha^2, \alpha\gamma, \gamma^2)$, so if $f \in \ker(\phi)$, $f(a,b,c) = f(\alpha^2, \alpha\gamma, \gamma^2) = \phi(f)(\alpha, \gamma) = 0$. Thus, $Z_K(\ker(\phi)) = Z_K((y^2 - xz))$, so $\sqrt{\ker(\phi)} = \sqrt{(y^2 - xz)}$. But $\ker(\phi)$ and $(y^2 - xz)$ are radical, so the claim holds in the algebraically closed case. In general, we observe that $S = K[x,y,z] \subseteq \overline{S} = \overline{K}[x,y,z]$ is faithfully flat. Then

$$\overline{S} \otimes_S \frac{\ker \phi}{(y^2 - xz)S} \cong \frac{(\ker \phi) \otimes \overline{S}}{(y^2 - xz)S \otimes \overline{S}} \cong \frac{\ker(\phi \otimes \overline{S})}{(y^2 - xz)\overline{S}} = 0$$

by the algebraically closed field case, so $\dfrac{\ker \phi}{(y^2 - xz)S} = 0$, establishing the claim in general. Now, $\text{frac}(K[u^2, uv, v^2]) = K(u^2, uv, v^2)$ has u^2, v^2 as a transcendence basis over K, so the dimension is 2.

Chapter 6

Dimension, locally

6.1 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 $K[x_1, \ldots, x_d]_{(x_1,\ldots,x_d)}$. We can consider this as the ring of rational functions that in lowest terms have a denominator with nonzero constant term. (We can talk about lowest terms since the polynomial ring is a UFD.)
6. Extending the following example, we have local rings like $(K[x_1, \ldots, x_d]/I)_{(x_1,\ldots,x_d)}$. If K is algebraically closed and I is a radical ideal, then $K[x_1, \ldots, x_d]/I = K[X]$ is the coordinate ring of some affine variety, and $(x_1, \ldots, x_d) = \mathfrak{m}_{\underline{0}}$ is the ideal defining the origin (as a point in $X \subseteq K^d$). Then we call $(K[x_1, \ldots, x_d]/I)_{(x_1,\ldots,x_d)} = K[X]_{\mathfrak{m}_{\underline{0}}}$ 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 $\underline{0}$.

We want to make a quick observation about local rings: let $(R, \mathfrak{m}, k)$ be local. Since k is a quotient of R, the characteristic of R must be a multiple of the characteristic of k; the kernel of the map from $\mathbb{Z}$ can only get bigger in the composition. Of course, with example 2 in mind, we must think of 0 as a multiple of any integer for this to make sense. Now k is a field, so its characteristic is 0 or p for a prime p. If $\mathrm{char}(k) = 0$, then necessarily $\mathrm{char}(R) = 0$. If $\mathrm{char}(k) = p$, we claim that $\mathrm{char}(R)$ must be either 0 or a power of p. Indeed, if we write $\mathrm{char}(R) = p^n \cdot m$ with m coprime to p, note that $p \in \mathfrak{m}$, so if $m \in \mathfrak{m}$, we have $1 \in (p, m) \subseteq \mathfrak{m}$, which is contradiction. Since R is local, this means that m is a unit. But then, $p^n m = 0$ implies $p^n = 0$, so the characteristic must be p^n. We summarize and add one more observation.

Proposition 6.4. *Let $(R, \mathfrak{m}, k)$ be a local ring. Then one of the following holds:*

1. $\mathrm{char}(R) = \mathrm{char}(k) = 0$. *We say that R has* equal characteristic zero.
2. $\mathrm{char}(R) = 0$, $\mathrm{char}(k) = p$ *for a prime p. We say that R has* mixed characteristic $(0, p)$.
3. $\mathrm{char}(R) = \mathrm{char}(k) = p$ *for a prime p. We say that R has* equal characteristic p.
4. $\mathrm{char}(R) = p^n$, $\mathrm{char}(k) = p$ *for a prime p and an integer $n > 1$.*

If R is reduced, then one of the first three cases holds.

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

Proposition 6.5. *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 $m_1, \ldots, m_s$ be a generating set for M. By assumption, we have equations

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

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 $m \in M$. □

Example 6.6. We will use this to give a quick proof of the fact that, if M is a finitely generated R-module, and $\varphi : M \to M$ is a surjective R-linear endomorphism, then φ is an isomorphism. In this setting, M is an $R[x]$-module by the rule $xm = \varphi(m)$, $x^2 m = \varphi^2(m)$, etc. The hypothesis that φ is surjective says that $xM = M$. Then, some element of (x) acts as the identity on M: $f(x)x$ is the identity, so $f(\varphi) \circ \varphi$ is the identity. Thus, φ is an isomorphism.

Proposition 6.7. *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 6.8. *Let $(R, \mathfrak{m}, k)$ be a local ring, and M be a finitely generated module. For $m_1, \ldots, m_s \in M$,*

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

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

Proof. The implication $\Rightarrow$ is clear. Let $N = \langle m_1, \ldots, m_s \rangle \subseteq M$. 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 6.9. *Let $(R, \mathfrak{m})$ be a local ring, and M a finitely generated module. A set of elements $\{m_1, \ldots, m_t\}$ is a* minimal generating set *of M if the images of $m_1, \ldots, m_t$ 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.

We now want to give graded analogues for the results above.

Proposition 6.10. *Let R be an $\mathbb{N}$-graded ring, and M a $\mathbb{Z}$-graded module such that $[M]_{<a} = 0$ for some a. If $M = (R_+)M$, then $M = 0$.*

In particular, if M is a finitely generated $\mathbb{Z}$-graded module and $M = (R_+)M$, then $M = 0$.

Proof. If M is finitely-generated, then it can be generated by finitely generated homogeneous elements (the homogeneous pieces of some finite generating set); thus the first statement implies the second.

M lives in degrees at least a, but $(R_+)M$ lives in degrees strictly bigger than a. If M has a nonzero element, it has a nonzero homogeneous element, and we obtain a contradiction. □

Just as above, we obtain the following:

Proposition 6.11. *Let R be an $\mathbb{N}$-graded ring, with R_0 a field, and M a $\mathbb{Z}$-graded module such that $[M]_{<a} = 0$ for some a. A set of elements of M generates M if and only if their images in $M/(R_+)M$ spans as a vector space. Since M and $(R_+)M$ are graded, $M/(R_+)M$ admits a basis of homogeneous elements.*

In particular, if K is a field, R is a positively graded K-algebra, and I is a homogeneous ideal, then I has a minimal generating set by homogeneous elements, and this set is unique up to K-linear combinations.

Note that we can use NAK to prove that certain modules are finitely generated in the graded case; in the local case, we cannot.

We want to prove one more important fact about Noetherian local rings. We prepare with a lemma.

17 Octubre

Lemma 6.12 (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 6.13 (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. □

6.2 Artinian rings

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 6.14. *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 $\mathfrak{m}_i R_{\mathfrak{m}_i}$-primary. Indeed, note that $(R/I)_{\mathfrak{m}_i} = R_{\mathfrak{m}_i}/IR_{\mathfrak{m}_i}$ has a unique maximal ideal $\mathfrak{m}_i R_{\mathfrak{m}_i}$. Thus, if $x, y \in R_{\mathfrak{m}_i}$ are such that $xy \in IR_{\mathfrak{m}_i}$, and $x \notin \mathfrak{m}_i R_{\mathfrak{m}_i}$, then x is a unit modulo $I_{\mathfrak{m}_i}$, so $y \in IR_{\mathfrak{m}_i}$. Then, the contraction of a primary ideal is primary (prove it!) 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 both sides are the unit ideal in $R_{\mathfrak{p}}$, otherwise, in $R_{\mathfrak{m}_i}$ they are proper but equal. Thus, the primary decomposition.

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. □

Definition 6.15. *A nonzero module is* simple *if it has no proper submodules. Equivalently, M is simple if it isomorphic to $R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.*

The nontrivial implication comes from the fact that any nonzero module contains a cyclic module, and if $M \cong R/I$ with I not maximal, we can surject to $R/\mathfrak{m}$ for a maximal ideal containing I, which has a proper kernel. Note already that if R is local, any simple module is isomorphic to the residue field.

Definition 6.16. *A module M has* finite length *if it has a filtration of the form*

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

with M_{i+1}/M_i simple for each i; such a filtration is called a composition series *of* length *n. We say a omposition series is* strict *if $M_i \neq M_{i+1}$ for all i. Two composition series are* equivalent *if the collections of composition factors M_{i+1}/M_i are the same up to reordering. The* length *of a finite length module M, denoted $\ell(M)$, is the minimum of the lengths of a composition series of M.*

We recall the Jordan-Holder theorem and some of its consequences:

Theorem 6.17 (Jordan-Holder theorem)**.**

- *For a module of finite length, any filtration can be refined to a composition series.*
- *For a module of finite length, any two composition series admit refinements that are equivalent.*
- *Every strict composition series for a fixed module of finite length is equivalent, and hence has the same length.*

Some basic consequences of this theorem for length include:

- If $M \subseteq N$, then $\ell(N) = \ell(M) + \ell(N/M)$. (Extend a composition series for M to one for N.)
- If $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$, then $\ell(M) = \sum_{i=0}^{n-1} \ell(M_{i+1}/M_i)$.
- If $M \subseteq N$, then $\ell(M) \leq \ell(N)$, with equality only if $M = N$.
- If M has finite length, then any *descending* chain of submodules of M stabilizes. Likewise, any *ascending* chain of submodule stabilizes.

Remark 6.18. We also note that if M is annihilated by a maximal ideal $\mathfrak{m}$, so that M is an $R/\mathfrak{m}$-module, the length of M is equal to its dimension as an $R/\mathfrak{m}$-vector space. In particular, $\ell(M/\mathfrak{m}M) = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

Example 6.19. Let $R = \mathbb{R}[x, y]_{(x,y)}$. Then $M = R/\mathfrak{m}^2$ has length 3, since we have a composition series $0 \subseteq xM \subseteq (x, y)M \subseteq M$; note that each is a copy of $R/\mathfrak{m}$. However, M is not an $R/\mathfrak{m}$-vector space.

Definition 6.20. *A ring is* Artinian *if every descending chain of ideals eventually stabilizes. A module is* Artinian *if every descending chain of submodules eventually stabilizes.*

Remark 6.21.

1. If R is an Artinian ring, then R/I is Artinian for any ideal I of R.
2. If R is an Artinian ring, then any nonempty family of ideals has a minimal element.
3. If M is an Artinian module, and $N \subseteq M$, then N and M/N are Artinian.

Theorem 6.22. *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 of Noetherian local rings, which 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 $\mathfrak{m} = (f_1, \ldots, f_t)$, with t finite since R is Noetherian, each $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is generated by $\{f_1^{a_1} \cdots f_t^{a_t} \mid a_1 + \cdots + a_t = i\}$ as a $(R/\mathfrak{m})$-vector space, hence has finite length, so the total length of R is finite.

(3)⇒(4): We have obsered this above.

(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.

Now, to see R is Noetherian, $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$ stabilizes again, so that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$; we can't apply NAK yet since we don't know $\mathfrak{m}^n$ is finitely generated. If $\mathfrak{m}^n \neq 0$, consider the family S of ideals $I \subseteq \mathfrak{m}$ such that $I\mathfrak{m}^n \neq 0$; this contains $\mathfrak{m}$. Just as the Noetherian property guarantees maximal elements of nonempty families, the Artinian property guarantees minimal elements; take J minimal in S. For some $x \in J$, $x\mathfrak{m}^n \neq 0$, and $(x) \subseteq J \subseteq \mathfrak{m}$, so $J = (x)$ is principal by minimality. Now, $x\mathfrak{m}(\mathfrak{m}^n) = x\mathfrak{m}^{n+1} = x\mathfrak{m}^n \neq 0$, so $x\mathfrak{m} \subseteq (x)$ is in the family S of ideals, and by minimality, $(x) = \mathfrak{m}(x)$. NAK applies to this, so $(x) = (0)$, contradicting that $\mathfrak{m}^n \neq 0$. Then, we have

$$0 = \mathfrak{m}^n \subseteq \mathfrak{m}^{n-1} \subseteq \cdots \subseteq \mathfrak{m} \subseteq R,$$

and since the Artinian property descends to submodules and quotients, each factor has finite length. Thus, R has finite length, so ideals in R satisfy ACC, as required. □

Example 6.23. Some Artinian local rings include $K[x,y]/(x^2, y^2)$, $K[x,y]/(x^2, xy, y^2)$, and $\mathbb{Z}/(p^n)$.

Example 6.24. Even though every Artinian ring is Noetherian and finite length, it is not true that Artinian modules are always Noetherian or finite length. Let $R = \mathbb{C}[\![x]\!]$, and $M = R[1/x]/R$. Note that $R[1/x]$ is the ring of Laurent series, so M is the module of "tails" of these functions. It does not have finite length; it is not even finitely generated! Observe that any submodule N of M either contains $1/x^n$ for all n, or else there is a largest n for which $1/x^n \in N$, and $N = R \cdot 1/x^n$ for this n. The module $R \cdot 1/x^n \subseteq M$ has length n, so is Artinian, thus M is Artinian.

29 Octubre

Proposition 6.25. *Let R be a Noetherian ring, and M be an R-module. M has finite length if and only if it is finitely generated and all of its associated primes are maximal ideals of R.*

Proof. If M has finite length, then it is Noetherian, hence finitely generated. Any composition series is a prime filtration, since the composition factors are cyclic quotients by maximal ideals, so all the associated primes of M must occur as factors in the composition series, hence every associated prime is maximal.

Conversely, if M is finitely generated, and every associated prime is maximal, then consider a prime filtration of M. Every factor in the prime filtration must contain an associated prime of M:

indeed, if $\mathfrak{q}$ is a composition factor that does not contain M, then $M_{\mathfrak{q}} = 0$ since $\mathrm{Ass}_{R_{\mathfrak{q}}}(M_{\mathfrak{q}}) = \varnothing$ by behavior of associated primes under localization, but we get a nonzero composition series of $M_{\mathfrak{q}}$ by localizing the composition series of M, which is a contradiction. Hence every composition factor must correspond to a maximal ideal, so this is a composition series. □

Definition 6.26. *If $(R, \mathfrak{m}, k)$ is local, a* coefficient field *for R is a subfield $K \subseteq R$ such that the map $K \to R \to R/\mathfrak{m} \cong k$ is an isomorphism.*

Rings like $K[\underline{x}]_{(\underline{x})}/I$ have coefficient fields: the copy of K. Some rings without coefficient fields are $\mathbb{Z}_{(p)}$, $\mathbb{R}[x]_{(x^2+1)}$. Some rings have lots of them: $\mathbb{C}[x, y]_{(x)}$ contains $\mathbb{C}(y)$ and $\mathbb{C}(x + y)$, which both are coefficient fields!

Remark 6.27. If $(R, \mathfrak{m}, k)$ is local with coefficient field K, then a finite length R-module M may not be a k-module (it may not be killed by $\mathfrak{m}$), but it is a K-vector space by restriction of scalars, and $\ell(M) = \dim_K(M)$.

6.3 Height and number of generators

Theorem 6.28 (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.*

We note that this is stronger than the statement that the height of (f) is at most one: we recall that that means that some 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 $\mathrm{ht}(\mathfrak{p}) > 1$, 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. □

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 6.29. *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 6.30 (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 $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}$ 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 $\mathfrak{p}_1\overline{R} \subsetneq \cdots \subsetneq \mathfrak{p}_h\overline{R}$ has length at most $h - 1 = n - 1$, and we will be done. 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 $\mathfrak{p} = \mathfrak{p}_{i-1}$. □

Example 6.31.

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 two, 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 $(u, v, w, x, y) = (I : x^2y^2)$, so I has an associated prime of height 5.

5. 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 $\operatorname{Min}(x) = \{\mathfrak{m}\}$. 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 $\operatorname{ht}(\mathfrak{m}) > 1$.

Lemma 6.32. *Let R be a Noetherian ring, and I be an ideal. Let $f_1, \dots, f_t \in I$, and $J_i = (f_1, \dots, f_i)$ for each i. If $f_i \notin \bigcup_{\mathfrak{a} \in \operatorname{Min}(J_{i-1}) \smallsetminus V(I)} \mathfrak{a}$ for each i, then any minimal prime of J_i either contains I, or else has height i.*

Proof. By induction on i. For $i = 0$, $J_0 = (0)$, and every minimal prime has height zero.

If we know the statement for $i = m$, consider a minimal prime $\mathfrak{q}$ of J_{m+1}. Since $J_m \subseteq J_{m+1}$, $\mathfrak{q}$ must contain a minimal prime of J_m, say $\mathfrak{p}$. If $\mathfrak{p} \supseteq I$, then $\mathfrak{q} \supseteq I$. If $\mathfrak{p}$ does not contain I, it has height m by the induction hypothesis. Then, $f_{m+1} \in J_{m+1}$ implies $f_{m+1} \in \mathfrak{q}$, but since $\mathfrak{p} \in \operatorname{Min}(J_m) \smallsetminus V(I)$, $f_{m+1} \notin \mathfrak{p}$, so $\mathfrak{q} \supsetneq \mathfrak{p}$. Thus, the height of $\mathfrak{q}$ is strictly greater than m, and by Krull height, it is then exactly $m + 1$. □

31 Octubre

Theorem 6.33. *Let R be a Noetherian ring of dimension d.*

1. *If $\mathfrak{p}$ is a prime of height h, then there are h elements $f_1, \ldots, f_h \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $(f_1, \ldots, f_h)$.*
2. *If I is any ideal in R, then there are (at most) $d+1$ elements $f_1, \ldots, f_{d+1} \in I$ such that $I = \sqrt{(f_1, \ldots, f_{d+1})}$.*
3. *If R is local or graded ($\mathbb{N}$-graded, with R_0 a field), and I is an ideal (homogeneous in the graded case), then there are d elements (homogeneous in the graded case) $f_1, \ldots, f_d \in I$ such that $I = \sqrt{(f_1, \ldots, f_d)}$.*

Proof. We will use the notation from the previous lemma.

1. If $\mathfrak{p}$ is a minimal prime, then we take the "empty sequence:" $\mathfrak{p}$ is minimal over (0). Otherwise, we will use the recipe from the lemma above, with $I = \mathfrak{p}$. We need to show that we can choose h elements satisfying the hypotheses, i.e., that $\mathfrak{p} \not\subseteq \bigcup_{\mathrm{Min}(J_i) \smallsetminus V(\mathfrak{p})} \mathfrak{a}$ for $i = 0, \ldots, h-1$. Note first that unless $i \geq h$, $\mathrm{Min}(J_i)$ cannot meet $V(\mathfrak{p})$, by Krull height, so $\mathrm{Min}(J_i) \smallsetminus V(\mathfrak{p}) = \mathrm{Min}(J_i)$ in the specified range. If $\mathfrak{p} \subseteq \bigcup_{\mathrm{Min}(J_i)} \mathfrak{a}$, then by prime avoidance, $\mathfrak{p}$ is contained in a minimal prime of J_i, which cannot happen for $i < h$. Thus, we can choose $(f_1, \ldots, f_h)$ as in the lemma, and its minimal primes have height h, or else contain $\mathfrak{p}$. Since $J_h = (f_1, \ldots, f_h) \subseteq \mathfrak{p}$, some minimal prime $\mathfrak{q}$ of J_h is contained in $\mathfrak{p}$. We know that this $\mathfrak{q}$ either contains $\mathfrak{p}$, and hence is $\mathfrak{p}$, or else is contained in and has the same height as $\mathfrak{p}$, so again must be equal to $\mathfrak{p}$.

2. Again, we use the recipe from above. We again need to see that we can do this. Inductively, we are choosing elements inside of I, so each J_i is contained in I, and $V(I) \subseteq V(J_i)$.

   If for some i we have $\mathrm{Min}(J_i) \smallsetminus V(I) = \varnothing$, then each minimal prime of J_i will lie in $V(I)$, so $V(J_i) \subseteq V(I)$, and equality holds, so the radicals are equal. If $\mathrm{Min}(J_i) \smallsetminus V(I) \neq \varnothing$, then $I \not\subseteq \mathfrak{q}$ for any $\mathfrak{q} \in \mathrm{Min}(J_i) \smallsetminus V(I)$, and $I \not\subseteq \bigcup_{\mathrm{Min}(J_i) \smallsetminus V(I)} \mathfrak{q}$ by prime avoidance, so we can choose elements as in the lemma.

   Thus, by the lemma, we either end up with $\sqrt{(f_1, \ldots, f_i)} = \sqrt{I}$ for $i \leq d$ or we get elements $(f_1, \ldots, f_{d+1}) = J_{d+1} \subseteq I$ such that the minimal primes contain I or have height at least $d+1$. In the latter case, by the assumption on the dimension, no prime has height $d+1$, so all the minimal primes of J_{d+1} contain I. But, since $J_{d+1} \subseteq I$, a minimal prime of J_{d+1} must also be minimal over I. Thus, $\mathrm{Min}(J_{d+1}) \subseteq \mathrm{Min}(I)$, so $V(J_{d+1}) \subseteq V(I)$, and equality holds, so the radicals are equal.

3. We run the same argument as in the last part (using homogeneous prime avoidance in the graded case). The point is that the only (homogeneous, in the graded case) ideal of height d already contains I. □

Corollary 6.34. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring. Then,*

$$\dim(R) = \min\{n \mid \exists f_1, \ldots, f_n : \sqrt{(f_1, \ldots, f_n)} = \mathfrak{m}\} \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

That is, the dimension of a Noetherian local ring is bounded by minimal the number of generators of its maximal ideal.

In particular, a Noetherian local ring has finite dimension.

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. The second inequality just follows from the fact that the right-hand quantity is the minimal number of generators of the ideal $\mathfrak{m}$. □

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 6.35. *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 $\sqrt{(x_1, \dots, x_d)} = \mathfrak{m}$.*

A sequence of d homogeneous elements $x_1, \dots, x_d$ in a d-dimensional $\mathbb{N}$-graded finitely generated K-algebra R, with $R_0 = K$, is a homogeneous system of parameters *if $\sqrt{(x_1, \dots, x_d)} = R_+$.*

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 Neotherian ring, or the height of a prime in a Noetherian ring. To help characterize systems of parameters, we pose the following definition:

Definition 6.36. *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 $\dim(R) \geq \dim(R/\mathfrak{p}) + \text{height}(\mathfrak{p})$.

Theorem 6.37. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $x_1, \dots, x_t \in \mathfrak{m}$.*

1. $\dim(R/(x_1, \dots, x_t)) \geq \dim(R) - t$.
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 $t + s \geq \dim(R)$.

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, hence has finite length, so $\text{Ass}_{R'}(R'/I) = \{\mathfrak{m}\}$, and I is $\mathfrak{m}$-primary in R'. Thus, $\dim(R')$ is equal to the height of I, which is then $\leq d - t$ by Krull height. That is, $\dim(R') \leq d - t$, 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. □

It is worth comparing the characterization in part three with our existence proof: we constructed a system of parameters by inductively avoiding all the minimal primes; a system a parameters is a sequence where we inductively avoid all of the absolutely minimal primes.

5 Diciembre

6.4 The dimension inequality

Our goal here is to prove a general inequality that we can think of as a generalization of the characterization of dimension of finitely generated algebras in terms of transcendence degree. Before we state and prove this, we give a generalization of our calculation of dimension of polynomial rings.

Theorem 6.38. *Let R be a Noetherian ring, $S = R[x]$ a polynomial ring in one variable over R, $\mathfrak{q} \in \mathrm{Spec}(S)$ and $\mathfrak{p} = \mathfrak{q} \cap R$. Then* $\mathrm{height}(\mathfrak{q}) \in \{\mathrm{height}(\mathfrak{p}), \mathrm{height}(\mathfrak{p}) + 1\}$*, and* $\mathrm{height}(\mathfrak{q}) = \mathrm{height}(\mathfrak{p})$ *if and only if $\mathfrak{q} = \mathfrak{p}S$.*

Proof. If the height of $\mathfrak{p}$ is at least h, take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h = \mathfrak{p}$ and expand to $\mathfrak{p}_0 R[x] \subsetneqq \cdots \subsetneqq \mathfrak{p}_h R[x] = \mathfrak{p}R[x] \subseteq \mathfrak{q}$. This is a chain of primes in S, so the height of $\mathfrak{q}$ is at least the height of $\mathfrak{p}$, and equality holds only if $\mathfrak{q} = \mathfrak{p}R[x]$.

Now, we can localize at $R \smallsetminus \mathfrak{p}$: this will not affect the height of $\mathfrak{p}$ or of $\mathfrak{q}$, since any prime contained in $\mathfrak{q}$ has empty intersection with this set. Thus, we assume $(R, \mathfrak{p})$ is local. Let $(f_1, \ldots, f_d)$ be a system of parameters for $\mathfrak{p}$. To show that $\mathrm{height}(\mathfrak{q}) \leq \mathrm{height}(\mathfrak{p}) + 1$, we want to show that there is some y such that $(f_1, \ldots, f_d, y)$ is a system of parameters for $R[x]_{\mathfrak{q}}$. Thus, it suffices to show that $R[x]_{\mathfrak{q}}/(x_1, \ldots, x_d)$ has dimension at most one. This ring is a localization of $(R/(f_1, \ldots, f_d))[x]$, so it suffices to show that this latter ring has dimenion at most one. The nilradical of this ring is the ideal $\mathfrak{p}[x]$, and quotienting out by this does not affect the dimension, so the dimension is the same as that of $R/\mathfrak{p}[x]$, which is one, since $R/\mathfrak{p}$ is a field.

If $\mathfrak{q} = \mathfrak{p}S$, we have $R[x]_{\mathfrak{q}}/(f_1, \ldots, f_d) \cong (R/(f_1, \ldots, f_d))[x]_{\mathfrak{p}[x]}$, and $\mathfrak{p}[x]$ consists of nilpotents in this ring, so it is the unique minimal prime; this localization has dimension zero. Thus, in this case, we have a system of parameters of the same size, so the heights are equal. □

Corollary 6.39. *If R is Noetherian, then* $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$.

Theorem 6.40. *Let $R \subseteq S$ be an inclusion of domains, with R Noetherian. Let $\mathfrak{q} \in \mathrm{Spec}(S)$ and $\mathfrak{p} = \mathfrak{q} \cap R \in \mathrm{Spec}(R)$. Then*

$$\mathrm{height}(\mathfrak{q}) + \mathrm{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \leq \mathrm{height}(\mathfrak{p}) + \mathrm{trdeg}(\mathrm{frac}(S)/\mathrm{frac}(R)).$$

Proof. **Case 1:** $S = R[s]$ is generated by one element.

Case 1(a): s is algebraically independent over R: Then S is isomorphic to a polynomial ring in the variable x, and $\mathrm{trdeg}(\mathrm{frac}(S)/\mathrm{frac}(R)) = 1$. Consider the fiber $\kappa_\phi(\mathfrak{p})$ of the inclusion ϕ: we compute $\kappa_\phi(\mathfrak{p}) = (R \smallsetminus \mathfrak{p})^{-1}\left(\frac{R[x]}{\mathfrak{p}R[x]}\right) \cong \kappa(\mathfrak{p})[x]$, which is a one-dimensional domain. Thus, either $\mathfrak{q}$ is minimal in $\kappa_\phi(\mathfrak{p})$, in which case $\mathfrak{q} = \mathfrak{p}R[x]$, or else $\mathfrak{q}\kappa_\phi(\mathfrak{p})$ is a maximal ideal and contains a nonzero polynomial in $\kappa(\mathfrak{p})[x]$; from the definitions we have

$$\frac{\kappa_\phi(\mathfrak{p})}{\mathfrak{q}\kappa_\phi(\mathfrak{p})} \cong \frac{(R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)}{\mathfrak{q}(R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)} \cong (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{q}),$$

and since this is a field (in the case $\mathfrak{q} \neq \mathfrak{p}R[x]$), it must agree with $\kappa(\mathfrak{q})$, so $\kappa(\mathfrak{q})$ is generated as a field over $\kappa(\mathfrak{p})$ by one algebraic element x. If $\mathfrak{q} = \mathfrak{p}R[x]$, then $\kappa(\mathfrak{q}) = \left(\frac{R[x]}{\mathfrak{p}R[x]}\right)_{\mathfrak{p}R[x]} \cong \kappa(\mathfrak{p})(x)$, so $\mathrm{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) = 1$, and in this case $\mathrm{height}(\mathfrak{q}) = \mathrm{height}(\mathfrak{p})$, so equality holds. Otherwise, we have $\mathrm{height}(\mathfrak{q}) = \mathrm{height}(\mathfrak{p}) + 1$ by the theorem above and $\mathrm{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) = 0$, so equality holds again.

Case 1(b): s is algebraic over R: Then $S \cong R[s] \cong R[x]/I$ for a nonzero prime I, and $\operatorname{trdeg}(\operatorname{frac}(S)/\operatorname{frac}(R)) = 0$. Since $I \cap R = 0$ and $I \neq 0$, the height of I is one, using the previous theorem. Let $\mathfrak{q}'$ be the primage of $\mathfrak{q}$ in $R[x]$, so $\mathfrak{q}' \cap R = \mathfrak{p}$. By the previous case, we know that

$$\operatorname{height}(\mathfrak{q}') + \operatorname{trdeg}(\kappa(\mathfrak{q}')/\kappa(\mathfrak{p})) = \operatorname{height}(\mathfrak{p}) + 1.$$

Then

$$\operatorname{height}(\mathfrak{q}') \geq \operatorname{height}(\mathfrak{q}) + \operatorname{height}(I) = \operatorname{height}(\mathfrak{q}) + 1,$$

and $\kappa(\mathfrak{q}') = \kappa(\mathfrak{q})$, so

$$\operatorname{height}(\mathfrak{q}) + \operatorname{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \leq \operatorname{height}(\mathfrak{q}') - 1 + \operatorname{trdeg}(\kappa(\mathfrak{q}')/\kappa(\mathfrak{p})) = \operatorname{height}(\mathfrak{p}),$$

as required.

Case 2: $S = R[s_1, \ldots, s_n]$ is finitely generated: inductively, and using case 1, we can assume we know the result for algebras with at most $n-1$ or 1 generators, let $T = R[s_1]$ and $\mathfrak{r} = \mathfrak{q} \cap T$. Since $S = T[s_2, \ldots, s_n]$, we have

$$\operatorname{height}(\mathfrak{q}) + \operatorname{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{r})) = \operatorname{height}(\mathfrak{r}) + \operatorname{trdeg}(\operatorname{frac}(S)/\operatorname{frac}(T)), \text{ and}$$

$$\operatorname{height}(\mathfrak{r}) + \operatorname{trdeg}(\kappa(\mathfrak{r})/\kappa(\mathfrak{p})) = \operatorname{height}(\mathfrak{p}) + \operatorname{trdeg}(\operatorname{frac}(T)/\operatorname{frac}(R)).$$

Since transencedence degree is additive for field extensions, this case follows.

Case 3: No finite generation assumption: if we localize at $R \smallsetminus \mathfrak{p}$, we do not affect heights or change fracton fields or residue fields, so we can assume that $(R, \mathfrak{p})$ is local. Let $h, t \in \mathbb{N}$ be such that $h \leq \operatorname{height}(\mathfrak{q})$ and $t \leq \operatorname{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ (both might be infinite). Take a chain of primes in S: $\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_h = \mathfrak{q}$. Let $y_1, \ldots, y_h$ be such that $y_i \in \mathfrak{q}_i \smallsetminus \mathfrak{q}_{i-1}$ and $z_1, \ldots, z_t \in S$ be such that the images in $\kappa(\mathfrak{q})$ are algebrically independent over $\kappa(\mathfrak{p})$. Let $S' = R[y_1, \ldots, y_h, z_1, \ldots, z_t] \subseteq S$ and $\mathfrak{q}' = \mathfrak{q} \cap S$. Note that $\operatorname{height}(\mathfrak{q}) \geq h$, and $\operatorname{trdeg}(\kappa(\mathfrak{q}')/\kappa(\mathfrak{p})) \geq t$. By Case 2, we have

$$h + t \leq \operatorname{height}(\mathfrak{q}') + \operatorname{trdeg}(\kappa(\mathfrak{q}')/\kappa(\mathfrak{p})) \leq \operatorname{height}(\mathfrak{p}) + \operatorname{trdeg}(\operatorname{frac}(S')/\operatorname{frac}(R)),$$

and since this holds for all $h \leq \operatorname{height}(Q)$ and $t \leq \operatorname{trdeg}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$, the claimed inequality holds. □

Corollary 6.41. *Let $R \subseteq S$ be domains, with R Noetherian. Then* $\dim(S) \leq \dim(R) + \operatorname{trdeg}(\operatorname{frac}(S)/\operatorname{frac}(R))$.

Proof. The height of a prime in S plus some nonnegative number is bounded above by the height of some other prime in R plus the transcendence degree. □

7 Diciembre

Chapter 7

Hilbert functions

7.1 Hilbert functions of graded rings

Definition 7.1. *If K is a field, the* Hilbert function *of an $\mathbb{N}$-graded K-algebra R is the function $H_R : \mathbb{Z} \mapsto \mathbb{N} \cup \infty$ 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.*

Example 7.2. Let K be a field, and $R = K[x, y]/(x^2, y^2)$. This ring has a K-vectors 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 7.3. Let K be a field, and $R = K[x_1, \ldots, x_n]$ be a polynomial ring with the standard grading: $|x_i| = 1$ for each i. To compute the Hilbert function, we need to compute the size of a K-basis for $H_R(t)$ for each t. We have

$$[R]_t = \bigoplus_{a_1+\cdots+a_n=t} K x_1^{a_1} \cdots x_n^{a_n}.$$

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.,

$$H_R(t) = \binom{t+n-1}{n-1} \quad \text{for } t \geq 0.$$

We observe the binomial function here can be expressed as a polynomial in t for $t \geq 0$; let

$$P_n(t) = \frac{(t+n-1)(t+n-2)\cdots(t+1)}{(n-1)!} \in \mathbb{Q}[t].$$

Observe that $P_n(t)$ has $-1, \ldots, -(n-1)$ as roots. Then we have

$$H_R(t) = \begin{cases} P_n(t) & \text{if } t > -n \\ 0 & \text{if } t < 0. \end{cases}$$

Note that the two cases overlap for $t = -(n-1), \ldots, -1$.

While the Hilbert function was a polynomial for $n \in \mathbb{N}$ in this example, this is not always the case.

Example 7.4. Let K be a field, and $R = K[x_0, \ldots, x_n]$ 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 $R' = K[x_1, \ldots, x_n]$ 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 $d \leq n$, then for all $i = 0, \ldots, d-1$ and all $t \geq 0$ 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 $t \geq 0$, so the Hilbert function agrees with a polynomial for all $t \geq 0$.

Now, we suppose that $d > n$, so $d - n - 1 \geq 0$. Using that $P_n(t) = H_{R'}(t)$ for $t \geq -n$ 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 7.5. *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 $d \leq n$, 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 $t \geq d - n$.*

We will see that the Hilbert function is always eventually equal to a polynomial, as in the last example. We prepare with a lemma.

Lemma 7.6. *Let R be a graded ring, and*

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

be a (degree-preserving) short exact sequence of graded R-modules. Then $H_M = H_L + H_N$.

Proof. 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. □

Recall that the dimension of a module M is the dimension of $R/\operatorname{ann}_R(M)$.

Theorem 7.7. *Let K be a field, and R be a finitely graded K-algebra such that $R_0 = K$ and R is generated by elements of degree one. 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 $t \geq n$. 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, we claim that $\operatorname{Ass}_R(M) = (R_+)$. Indeed, under these hypotheses, every homogeneous ideal is contained in R_+, since it is the ideal generated by all homogeneous elements. Since every associated prime is homogeneous, it must be contained in R_+. If some other homogeneous prime $\mathfrak{p}$ is associated to M, we have $\dim(R/\mathfrak{p}) \geq 1$, and $R/\mathfrak{p} \hookrightarrow M$ contradicts the hypothesis on dimension. Since M is finitely generated and its only associated prime is maximal, 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. Take a homogeneous prime filtration of M:

$$M = M_m \supsetneq M_{m-1} \supsetneq M_{m-2} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

with $M_i/M_{i-1} \cong R/\mathfrak{p}_i(d_i)$ for some homogeneous primes $\mathfrak{p}_i$ and integers d_i. Using the lemma inductively on i, we get that $H_M(t) = H_{R/\mathfrak{p}_1(d_1)}(t) + \cdots + H_{R/\mathfrak{p}_m(d_m)}(t)$. Observe that $H_{R/\mathfrak{p}_i(d_i)}(t) = H_{R/\mathfrak{p}_i}(t + d_i)$ for each i. Since the associated primes of M are contained in $V(\operatorname{ann}_R(M))$, we have $\dim(R/\mathfrak{p}_i) \leq \dim(M)$, and there must be some $\mathfrak{p}_i$ for which equality occurs, since every associated prime of M occurs, and the minimal primes of $\operatorname{ann}_R(M)$ are associated to M. If we can show that each module of the form $R/\mathfrak{p}_i$ verifies the conclusion of the theorem, then we are done: all of the claims of polynomiality, degree, and positivity of leading term pass to $H_M(t)$ by the equality above, as the shifting does not change degree or the leading term, $\dim(M) = \max\{\dim(R/\mathfrak{p}_i)\}$, and the leading term satisfies the hypotheses again.

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. Every factor is either a shift of A, or else has dimension less than $a := \dim(A) = \dim(M)$, since A is a domain. Applying the induction hypothesis and the formula $H_M(t) = H_{R/\mathfrak{p}_1(d_1)}(t) + \cdots + H_{R/\mathfrak{p}_m(d_m)}(t)$ from above 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. Thus, the claim holds for M, and hence in general as our induction is complete. □

12 Diciembre

Definition 7.8. *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 7.9. *Let K be a field, and R be a finitely graded K-algebra such that $R_0 = K$ and R is generated by elements of degree one. Let $0 \to L \to M \to N \to 0$ be a 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 7.10. 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 can compute this using the previous lemma plus the Noether normalization.

We also want to consider the case when the ring is not necessarily generated in degree one. The key fact we will use is the following.

Proposition 7.11. *Let K be a field, and R be a finitely-generated positively graded K-algebra with $R_0 = K$. Then there is some $d \in \mathbb{N}$ such that the subring $R^{(d)} = \bigoplus_{i\in\mathbb{N}}[R]_{id}$ is generated as a K-algebra by $[R]_d$.*

Proof. Exercise. □

The definition we need to generalize our results is the following.

Definition 7.12. *A function $f : \mathbb{Z} \to \mathbb{R}$ is called a* quasipolynomial *if there is an integer b and polynomials $p_0, \dots, p_{b-1} \in \mathbb{R}[t]$ such that $f(n) = p_c(n)$ for $c \equiv n \bmod b$ for each $n \in \mathbb{Z}$.*

Theorem 7.13. *Let K be a field, and R be a finitely graded K-algebra such that $R_0 = K$. Let M be a finitely generated graded R-module. Then there is a quasipolynomial where each coefficient has rational coefficients $P_M(t)$ such that $H_M(t) = P_M(t)$ for $t \gg 0$.*

Proof. Let d be such that $R^{(d)}$ is generated by $[R]_d$. Thus, we can think of $R^{(d)}$ as a standard graded K-algebra, if we consider the elements of $[R]_{id}$ to have degree i. Since R is finitely generated as a K-algebra, it is certainly a finitely generated $R^{(d)}$-algebra. Furthermore, any element $x \in R$ satisfies a monic equation of the form $t^d - x^d \in R^{(d)}[t]$, so R is integral and module-finite over $R^{(d)}$. Thus, M is a finitely generated $R^{(d)}$-module. However, its grading over R is not consistent with the grading of $R^{(d)}$. We can decompose M as an $R^{(d)}$-module as

$$M = M_0 \oplus M_1 \oplus \cdots \oplus M_{d-1}, \quad \text{where } M_j = \bigoplus_{i\in\mathbb{N}} [M]_{j+id}.$$

Then, setting $[M_j]_i = [M]_{j+id}$, we obtain a grading on each M_j that is compatible with $R^{(d)}$. Note also, that each M_j is a submodule of a finitely generated module over a Noetherian ring, so is also finitely generated. Then, each M_j admits a Hilbert polynomial. Taking each of these, we obtain a quasipolynomial that agrees with the Hilbert function for large values. □

7.2 Associated graded rings and general Hilbert functions

Definition 7.14. *Let $(R, \mathfrak{m})$ be a local ring. The Hilbert function of R is the function $H_R(t) = \ell_R(\mathfrak{m}^t/\mathfrak{m}^{t+1})$.*

This function has similar properties to the Hilbert function for graded rings. To see this, we will use the notion of the associated graded ring.

Definition 7.15. *The* associated graded ring *of an ideal I in a ring R is the ring $\operatorname{gr}_I(R) := \bigoplus_{n\in\mathbb{N}} I^n/I^{n+1}$, with n-th graded piece I^n/I^{n+1}, and multiplication $(a + I^{n+1})(b + I^{m+1}) = ab + I^{m+n+1}$ for $a \in I^n, b \in I^m$. If $(R, \mathfrak{m})$ is local, then $\operatorname{gr}(R) := \operatorname{gr}_{\mathfrak{m}}(R)$.*

Note that the multiplication is well-defined. We observe also from the definitions that $[\mathrm{gr}_I(R)]_0 = R/I$, so if $(R, \mathfrak{m}, k)$ is local then $[\mathrm{gr}(R)]_0 = k$, and $\mathrm{gr}_I(R)$ is generated as a $[\mathrm{gr}(R)]_0$-algebra by elements of degree one. Again by the definitions, we have that for $(R, \mathfrak{m})$ local, $H_R(t) = H_{\mathrm{gr}(R)}(t)$. To get a completely satisfactory analogue of the Hilbert function theory in this setting, we would like to undertand the dimension of the associated graded ring. To understand this, we use the following related object.

Definition 7.16. *Let R be a ring, and I an ideal. The* Rees ring *of I is the $\mathbb{N}$-graded ring $R[It] \subseteq R[t]$, and the* extended Rees ring *of I is the $\mathbb{Z}$-graded ring $R[It, t^{-1}] \subseteq R[t, t^{-1}]$. In both cases, the grading is given by setting $|t| = 1$, and $|r| = 0$ for all $r \in R$.*

To understand these rings better, we write out the graded pieces. We have

$$R[It] = R \oplus It \oplus I^2t^2 \oplus \cdots \qquad \text{and} \qquad R[It, t^{-1}] = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus R \oplus It \oplus I^2t^2 \oplus \cdots .$$

Note that $t \notin R[It, t^{-1}]$ since $1 \notin I$, so t^{-1} is not a unit, even though it looks like one.

Lemma 7.17. *There are isomorphisms $R[It, t^{-1}]/(t^{-1}) \cong \mathrm{gr}_I(R)$ and $R[It, t^{-1}]/(t^{-1} - 1) \cong R$.*

Proof. For the first isomorphism, since t is homogeneous, we can use the graded structure. We have

$$t^{-1}R[It, t^{-1}] = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus I \oplus I^2t \oplus I^3t^2 \oplus \cdots ,$$

and matching the graded pieces, we find that the claimed isomorphism holds.

For the second isomorphism, we consider the map $R[It, t^{-1}] \to R$ given by sending $t \mapsto 1$. This is surjective, and the kernel is the set of elements $a_m t^m + \cdots + a_n t^n$ such that $a_m + \cdots + a_n = 0$. We claim that this ideal is generated by $(t^{-1} - 1)$. We proceed by induction on $n - m$. The case $n - m = 0$ corresponds to there being at most one nonzero term, in which case any element in the kernel is zero, and the claim trivially holds. In $n-m = 1$, we have an element of the form $at^{n-1} - at^n$ for some a, which is of the form $(at^n)(t^{-1} - 1)$. For the inductive step, if $a_m + \cdots + a_n = 0$, write $a_m t^m + \cdots + a_n t^n = (a_m t^m + \cdots + (a_{n-1} + a_n)t^{n-1}) + (-a_n t^{n-1} + a_n t^n)$. Observe that the set of coefficients in $R[It, t^{-1}]$ of t^n is a subset of the set of coefficients of t^{n-1} so both terms in parentheses live in $R[It, t^{-1}]$, and they are clearly in the kernel of the evaluation map. The inductive hypothesis applies to each term in parentheses, so we are done. □

Lemma 7.18. *If R is a Noetherian ring, and I an ideal, then the minimal primes of $R[It, t^{-1}]$ are exactly the primes of the form $\mathfrak{p}R[t, t^{-1}] \cap R[It, t^{-1}]$ for $\mathfrak{p} \in \mathrm{Min}(R)$.*

Proof. Write $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$, a minimal primary decomposition of (0) in R, and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. It is easy to see that $\mathfrak{q}_i R[t]$ is primary with radical $\mathfrak{p}_i R[t]$ (check it!). Then the same is true in $R[t, t^{-1}]$, by localizing. Contracting to $R[It, t^{-1}]$, we get primary ideals that intersect to (0); none is contained in the intersection of the others, since this is the case after intersecting with R, and likewise the radicals are distinct since they contract to different primes in R.

Thus setting $\mathfrak{q}_i' = \mathfrak{q}_i R[t, t^{-1}] \cap R[It, t^{-1}]$, $\mathfrak{q}_1' \cap \cdots \cap \mathfrak{q}_t'$ is a minimal primary decomposition of (0) in $R[It, t^{-1}]$. □

Theorem 7.19. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $I \subseteq \mathfrak{m}$ an ideal. Then* $\dim(R) = \dim(R[It, t^{-1}]) - 1 = \dim(\mathrm{gr}_I(R))$.

Proof. By the previous lemma, we can reduce to the case that R is a domain for the first equality. Observe that $\mathrm{trdeg}(\mathrm{frac}(R[It, t^{-1}])/\mathrm{frac}(R)) = \mathrm{trdeg}(\mathrm{frac}(R)(t)/\mathrm{frac}(R)) = 1$, so by the dimension inequality, $\dim(R[It, t^{-1}]) \leq \dim(R) + 1$.

Now, we claim that

$$Q = \cdots \oplus Rt^{-2} \oplus Rt^{-1} \oplus \mathfrak{m} \oplus It \oplus I^2t^2 \oplus \cdots = (\mathfrak{m}, It, t^{-1})R[It, t^{-1}]$$

is a maximal ideal of height $\dim(R) + 1$ in $R[It, t^{-1}]$. The quotient ring is $R/\mathfrak{m}$, so it is clearly maximal. Given a chain $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h = \mathfrak{m}$, of length $h = \dim(R)$, let $\mathfrak{q}_i = \mathfrak{p}_i R[t, t^{-1}] \cap R[It, t^{-1}]$. Since $\mathfrak{q}_i \cap R = \mathfrak{p}_i[t, t^{-1}] \cap R = \mathfrak{p}_i$ this is a proper chain of primes in $R[It, t^{-1}]$. We have

$$\mathfrak{q}_h = \cdots \oplus \mathfrak{m}t^{-2} \oplus \mathfrak{m}t^{-1} \oplus \mathfrak{m} \oplus It \oplus I^2t^2 \oplus \cdots = (\mathfrak{m}, It)R[It, t^{-1}] \subsetneqq Q$$

so the height of Q is at least $\dim(R) + 1$, and hence equal to $\dim(R) + 1$ using the previous upper bound on the dimension.

For the last equality, since t^{-1} is a nonzerodivisor on $R[It, t^{-1}]$, we have $\dim(\mathrm{gr}_I(R)) \leq \dim(R[It, t^{-1}]) - 1$. For the other inequality, let $\overline{Q} = Q/(t^{-1})$. Then

$$\dim(\mathrm{gr}_I(R)) \geq \dim(\mathrm{gr}_I(R)_{\overline{Q}}) = \dim(R[It, t^{-1}]_Q/(t^{-1}))$$

$$\geq \dim(R[It, t^{-1}]_Q) - 1 = \mathrm{height}(Q) - 1 = \dim(R). \qquad \square$$

We now can summarize the behavior of Hilbert functions of local rings.

Theorem 7.20. *Let $(R, \mathfrak{m}, k)$ be a local ring. Then there is a polynomial $P_R(t) \in \mathbb{Q}[t]$ of degree equal to $\dim(R) - 1$ such that $H_R(t) = P_R(t)$ for $t \gg 0$, and $(\dim(R) - 1)!$ times the leading coefficient is a positive integer, called the* multiplicity *of R.*

Proof. This follows from the equalities $H_R(t) = H_{\mathrm{gr}(R)}(t)$ and $\dim(R) = \dim(\mathrm{gr}(R))$, and that $\mathrm{gr}(R)$ is an $\mathbb{N}$-graded k-algebra with degreee zero piece equal to k and finitely generated by elements of degree one. $\square$

Index