1 Groebner Bases

Diane Maclagan
Hill 240 maclagan@math
Office Hour M1-2
Text: Eisenbud, recommended: Atiyah-Macdonald
Outline:
Gröbner Bases
Localization
Associated Primes
Integral Dependence
Blow-ups/filtrations
Flatness
Completion
Dimension
CM rings
<u>Gröbner Basics</u>

Definition 1.1 (Affine Variety)**.** *Let $S = k[x_1, \ldots, x_n]$ and let I be an ideal of S. Fact: S is Nötherian so $I = \langle f_1, \ldots, f_k \rangle$.*

The affine variety $V(I) = \{\underline{v} = (v_1, \ldots, v_n) \in k^n : f(\underline{v}) = 0 \forall f \in I\} = \{\underline{v} \in k^n : f_i(\underline{v}) = 0, 1 \leq i \leq k\}$.

For example, $S = k[x, y]$ and $I = \langle x - y \rangle$ gives the line $y = x$ and $V(y^2 - x^3 + x)$ is an elliptic curve.

Definition 1.2 (Projective Space)**.** *Projective space, $\mathbb{P}^n_k$ is the set of lines through the origin in k^{n+1}. We write a point in $\mathbb{P}^n$ as $\underline{v} = (v_0 : \ldots : v_n)$ and $\underline{v} \sim \underline{v}'$ if $\underline{v} = \lambda \underline{v}'$ for some $\lambda \in k^*$.*

Definition 1.3 (Projective Variety)**.** *If we set $S = k[x_0, \ldots, x_n]$, and grade S by $\deg(x_i) = 1$ for $0 \leq i \leq n$, then a polynomial is homogeneous if every monomial has the same degree. In fact, if $f \in S$ is homogeneous of degree d, we can ask if $f(\vec{v}) = 0$ for $\vec{v} \in \mathbb{P}^n$, because $f(\lambda \vec{v}) = \lambda^d f(\vec{v})$.*

A Projective Variety is $V(I) = \{\vec{v} \in \mathbb{P}^n : f(\vec{v}) = 0 \forall f \in I$ homogeneous $\}$

So, we ask the question, given $I \subset k[x_1, \ldots, x_n] = S$, $f \in S$ is $f \in I$? ie, if $I = \langle f_1, \ldots, f_r \rangle$, are there $h_1, \ldots, h_r \in S$ with $f \in \sum_{i=1}^r h_i f_i$.

e.g., is $x + 7 \in \langle x^2 - 4x + 3, x^2 + x - 2 \rangle \subset k[x]$? Well, $k[x]$ is a PID, so $I = \langle f \rangle$ for some $f \in k[x]$, and $x + 7 \in I$ iff $f | (x + 7)$. So we use the Euclidean Algorithm.

The Euclidean Algorithm gives $x - 1$ as the gcd, so $I = (x - 1)$, so $x + 7 \notin I$ as $x - 1 \not| x + 7$.

How about in several variables? Is $x + 3y - 2z \in \langle x + y - z, y - z \rangle$, ie, is $(1, 3, -2) \in \langle (1, 1, -1), (0, 1, -1) \rangle$? We can use Gaussian Elimination to say no.

Now, is $xy^2 - x$ in $\langle xy + 1, y^2 - 1 \rangle$? Naive attempts at division don't work, but $xy^2 - x = x(y^2 - 1)$, so it IS in the ideal.

Definition 1.4 (Gröbner Basis (Vague)). *A Gröbner Basis for an ideal I is a generating set for which long division decides the ideal membership problem.*

Definition 1.5 (Term Order). *A term order is a total order on the monomials in $S = k[x_1, \ldots, x_n]$ such that*

1. $1 < x^u := x_1^{u_1} \ldots x_n^{u_n}$ *for all* $\underline{u} \in \mathbb{N}^n \setminus \{0\}$
2. $x^u < x^v \Rightarrow x^{u+w} < x^{v+w}$.

Examples include lexicographic ordering, that is, $x^u < x^v$ if the first entry of $v - u$ is positive, for example $y^7 < xz^2 < x^2$.

Graded lex, $x^u < x^v$ if $\deg(x^u) < \deg(x^v)$ or $\deg(x^u) = \deg(x^v)$ and $x^u <_{lex} x^v$.

Reverse Lex (degree revlex), $x^u < x^v$ if $\deg(x^u) < \deg(x^v)$ or the last nonzero element of $v - u$ is negative. eg, $xz < y^2 < z^3$.

Definition 1.6 (Lead Term, Initial Ideal). *The leading term of a polynomial $f \in I$ is the largest monomial appearing in it with respect to a term order, e.g. $f = 3x^2 - 7xy + 8z^2$ with lex gives $in_<(f) = x^2$.*

The initial ideal $in_<(I) = \langle in_<(f) : f \in I \rangle$. WARNING: if $I = \langle f_1, \ldots, f_r \rangle$, then $in_<(I) \supseteq \langle in(f_1), \ldots, in(f_r) \rangle$ but they are not, in general, equal.

eg, $I = \langle xy + 1, y^2 - 1 \rangle$, $x + y \in I$, $y(xy + 1) - x(y^2 - 1)$, so if $<$ is lex, $in(x + y) = x \in in(I) \neq \langle xy, y^2 \rangle$.

Definition 1.7 (Gröbner Basis). *A Gröbner Basis for $I \subset S$ is a generating set $\mathscr{G} = \{g_1, \ldots, g_s\}$ for I for which $in(I) = \langle in(g_1), \ldots, in(g_S) \rangle$.*

Point: We can define a division algorithm. Order the Gröbner basis and divide the polynomial by multiplying elements of the Gröbner basis to cancel the leading term of f if possible, otherwise pass to the next monomial, etc.

If $\mathscr{G}$ is a Gröbner basis, then division by $\mathscr{G}$ will have remainder 0 if and only if the polynomial is in the ideal.

Facts: Every ideal in $k[x_1, \ldots, x_n]$ has a (finite) Gröbner basis, and there exists an algorithm called the Buchberger Algorithm to compute it.

Definition 1.8 (Division Algorithm). *Input: f, $\{g_1, \ldots, g_k\}$*

Output: Remainder on dividing f by $\{g_1, \ldots, g_k\}$.

Set $f' = f$, $r = 0$. While $in(f') \in \langle in(g_1), \ldots, in(g_k) \rangle$, let j be the smallest index for which $in(f') = x^u in(g_j)$. Set $f' = f' - lc(f')/lc(g_j) x^u g_j$

If $f' = 0$, return r otherwise $r = r + lc(f') in(f')$ and $f' = f' - lc(f') in(f')$, and return to the while loop.

Note: this algorithm terminates because a term order has no infinite descending chains. Also, this algorithm writes $f = \sum h_i g_i + r$ for some polynomials $h_i \in S$ with $in(h_i g_i) \leq in(f)$.

Proposition 1.1. *If $\mathscr{G} = \{g_1, \ldots, g_s\}$ is a Gröbner basis for I then the remainder on dividing f by $\mathscr{G}$ is 0 iff $f \in I$.*

Proof. If $r = 0$ then $f \in I$ since $f = \sum h_i g_i$.

Conversely, if $f \in I$, then in the while lop, $f' \in I$ and we only leave it when $f' = 0$, so $r = 0$. $\square$

Definition 1.9 (S-Pair)**.** *If $f, g \in S$ their S-pair is $S(f,g) = \frac{\mathrm{lcm}(in(f),in(g))}{lc(f)in(f)} f - \frac{\mathrm{lcm}(in(f),in(g))}{lc(g)in(g)} g$.*

eg, if $f = 3x^2 - 7y^2$ and $g = 8xy + z^2$, so $S(f,g) = \frac{x^2y}{3x^2}(3x^2 - 7y^2) - \frac{x^2y}{8xy}(8xy + z^2) = -\frac{7}{3}y^3 - \frac{1}{8}xz^2$.

The S is for syzygy.

Algorithm 1 (Buchberger)**.** *Input: $\{f_1, \ldots, f_s\}$ generating I, and a term order $<$.*

Output: A Gröbner basis for I wrt $<$.

1. *Current=$\{(f_i, f_j) : 1 \leq i < j \leq s\}$, $\mathscr{G} = \{f_1, \ldots, f_s\}$*
2. *While Current$\neq \emptyset$, do Pick $(f,g) \in$Current, Current=Current$\setminus(f,g)$, $r =$remainder on dividing $S(f,g)$ by $\mathscr{G}$. If $r \neq 0$, then $\mathscr{G} = \mathscr{G} \cup \{r\}$ and Current=Current$\cup\{(r,f) : f \in \mathscr{G}\}$.*
3. *Output $\mathscr{G}$*

Corollary 1.2. *If $\{g_1, \ldots, g_s\} \subset I$ and $\langle in(g_1), \ldots, in(g_s)\rangle = in(I)$ then $\{g_1, \ldots, g_s\}$ generate I.*

Definition 1.10 (Minimal Gröbner Basis)**.** *A GB is minimal if each $in(g_i)$ is a minimal generator of $in(I)$ and each minimal generator appears once in $\{in(g_i)\}$.*

Definition 1.11 (Reduced Gröbner Basis)**.** *A Gröbner basis is reduced if for all $g \in \mathscr{G}$ remainder on dividing g by $\mathscr{G} \setminus \{g\}$ is g.*

Example: There is a unique reduced GB for each term order.

Proof. We must check that Buchberger's Algorithm terminates and gives the correct answer.

At stage i of the algorithm, set $I_i = \langle in(g) : g \in \mathscr{G}\rangle$. Note that $I_{i+1} \supsetneq I_i$. If the algorithm did not terminate, we would get an infinite ascending chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$ which would contradict the fact that S is Nötherian.

If the output is not a Gröbner basis, then there is $f \in I$, $f = \sum h_i g_i$ with $g_i \in \mathscr{G}$, $h_i \in S$ with $in(f) \notin \langle in(g) : g \in \mathscr{G}\rangle$. Write $m = \max in(h_i g_i)$, we will assume that m is minimal for such a counterexample. Let $\mathscr{I}_m = \{i : in(h_i g_i) = m\}$, since $m \in \langle \in (g) : g \in \mathscr{G}\rangle$, we must have $in(f) < m$. Thus, $|\mathscr{I}_m| \geq 2$. Second assumption, $\mathscr{I}_m$ is minimal for such expressions.

Pick $i, j \in \mathscr{I}$. Write $S(g_i, g_j) = \sum p_j g_k$, $p_k \in S$. Since $in(g_i), in(g_j) | m$, $lcm(in(g_i), in(g_j)) | m$, so there exit $c \in k, m'$ monomial such that $in(cm'\ell_i g_i) = in(h_i g_i) = in(cm' l_j g_j)$, so $cm\ell_i g_i = cm'(\ell_j g_j + \sum p_k g_k)$, where $in(cm' p_k g_k) = m' in(p_k g_k) < m$.

Replace $h_i g_i + h_j g_j$ by $(h_i - cm'\ell_i)g_i$ which has initial term $< m$ as does $(h_j + cm'\ell_j)g_j$, so $\sum cm' p_k g_k$ has initial term $< m$.

This gives either a set with smaller $|\mathscr{I}_m|$ or smaller m, contradicting our minimality assumption. $\square$

Applications of the Division Algorithm

1. Given $I \subset k[x_1, \ldots, x_n]$, compute $I \cap k[x_2, \ldots, x_n] = I'$. $V(I') \subset k^{n-1}$ is the closure of the projection of $V(I)$ to k^{n-1}. The algorithm is to compute a lex GB for I with x_1 largest and take the polynomials without x_1 in them.

2. As $V(I \cap J) = V(I) \cup V(J)$, we may want to compute $I \cap J$. Compute $K = tI + (1-t)J \subset S[t]$, then compute $K \cap S$.

3. $I : J = \langle f | fg \in I$ for all $g \in J \rangle$. This is, geometrically, the closure of $V(I) \setminus V(J)$. $I : J = \cap(I : f_i)$ where $J = \{f_1, \ldots, f_s\}$, and $I : f$ is computed by computing $I \cap (f)$ and then dividing the generating set by f.

2 Hom, Tensor and Localization

Definition 2.1 ($\hom_R(M,N)$)**.** *$\hom_R(M,N)$ is the set of R-module homomorphisms from M to n, ie, $\varphi : M \to N$ is a group homomorphism with $\varphi(rm) = r\varphi(m)$. It is, in fact, a group with $(\phi + \psi)(m) = \phi(m) + \psi(m)$, and has an R-module structure by $(r\phi)(m) = r(\phi(m))$.*

This means $\hom_R(M, -)$ is a covariant functor from R-mod to R-mod. The map on objects takes N to $\hom_R(M,N)$. If $\alpha : N \to N'$ is an R-module homomorphism, then $\hom_R(M,\alpha) : \hom_R(M,N) \to \hom_R(M,N')$ by $\phi \mapsto \alpha \circ \phi$. Similarly, $\hom_R(-,N)$ is a contravariant functor from R-mod to R-mod.

Proposition 2.1. hom *is left exact. That is, if $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ then $0 \to \hom_R(M,A) \xrightarrow{\hom_R(M,\alpha)} \hom_R(M,B) \xrightarrow{\hom_R(M,\beta)} \hom_R(M,C)$.*

WARNING: If $0 \to A \to B \to C \to 0$, we don't expect $0 \to \hom_R(M,A) \to \hom_R(M,B) \to \hom_R(M,C) \to 0$ to be exact.

Example: $0 \to \mathbb{Z} \xrightarrow{x2} \mathbb{Z} \to \mathbb{Z}/2 \to 0$, apply $\hom(\mathbb{Z}/2, -)$. This is where Ext comes from.

In general, $0 \to A \to B \to C \to 0$ and if F is a functor, you don't expect $0 \to F(A) \to F(B) \to F(C) \to 0$ to be exact. If f is left (right) exact we get derived functors from taking cohomology.

<u>Tensor Product</u>

Definition 2.2 (Tensor)**.** *If M, N are R-modules then $M \otimes_R N$ is the abelian group that is the quotient of the free abelian group on the symbols $\{m \otimes n : m \in M, n \in N\}$ modulo the relations $(am + bm') \otimes (cn + dn') = acm \otimes n + adm \otimes n' + bcm' \otimes n + bdm' \otimes n'$. It is an R-module by $r(m \otimes n) = rm \otimes n = m \otimes rn$.*

Remember, not everything in $M \otimes N$ is of the form $m \otimes n$.

Example: What are the elements in $k^{mn} = k^m \otimes_k k^n$ of the form $m \otimes n$? The answer is the rank 1 matrices. These can be written as uv^T where $u \in k^m$ and $v \in k^n$.

$\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$ since $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$.

Change of coefficients: $k[x] \otimes_k R \simeq R[x]$ when R is a k-algebra.

Proposition 2.2. *The tensor product satisfies the following universal property: if φ a bilinear map $\varphi : M \times N \to P$ that is bilinear, then there exists a unique $\tilde{\varphi}$ such that*

$$\begin{tikzcd} M \times N \arrow[r] \arrow[dr, "\varphi"'] & M \otimes N \arrow[d, "\tilde{\varphi}"] \\ & P \end{tikzcd}$$

<u>Geometric Interpretation</u>

Given $X \subseteq k^n$, we can form $I(X) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \forall x \in X\}$. Hilbert's Nullstellensatz says that if k is algebraically closed, then $I(V(I)) = \sqrt{I}$.

Coordinate ring of a variety V is $S/I(V)$, and maps of varieties correspond to maps of rings in the other direction (see algebraic geometry for details).

If M is the coordinate ring of V, N is for U and R is for W. If $f : V \to W$ and $g : U \to W$, then the fiber product of V and U over W is $F = \{(u, v) \in U \times V : f(u) = g(v)\}$. The universal property it satisfies is that $\varphi : Z \to U \times V$ such that $f \circ \pi_1 \circ \varphi = g \circ \pi_2 \circ \varphi$ then

$$\begin{tikzcd} Z \arrow[dd, dashed] \arrow[dr, "\exists!"] \arrow[ddr, "\pi_2"] & \\ & U \times V \arrow[dl, "\pi_1"'] \arrow[dr] \\ U \arrow[dr, "f"'] & F \\ & W \end{tikzcd} \qquad \begin{tikzcd} & V \arrow[dl, "g"] \\ W & \end{tikzcd}$$

Point: the map $V \to W$ gives a map $R \to M$ which makes M an R-module by $rm = \varphi(r)m$.

Claim: $M \otimes_R N$ is the coordinate ring of the fiber product f, eg, $k[x_1, \ldots, x_n] \otimes_k k[y_1, \ldots, y_m] \simeq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

Claim: $- \otimes_R M$ is a right exact functor from R-mod to R-mod.

If $\varphi : M \to M'$, then $\varphi \otimes N : M \otimes_R N \to M' \otimes_R N$ comes from the bilinear map $\psi : M \times N \to M' \otimes N$ by $\psi(m, n) = \varphi(m) \otimes_R n$.

Now we check right exactness. Suppose $A \to B \to C \to 0$ is exact. We want to show that $A \otimes_R N \overset{\alpha\otimes 1}{\to} B \otimes_R N \overset{\beta\otimes 1}{\to} C \otimes_R N \to 0$. To see that $\beta \otimes 1$ is surjective, note that if $c \otimes n \in C \otimes N$ then there is $b \in B$ with $\beta(b) = c$, so $\beta \otimes 1(b \otimes n) = c \otimes n$.

To show that the other step is exact, we'll show that $C \otimes N \simeq B \otimes_R N/\alpha \otimes 1(A \otimes_R N)$. We'll do this by checking that $B \otimes N/A \otimes N$ satisfies the universal property of $C \otimes N$. Suppose that $\varphi : C \times N \to P$ is a bilinear map with $\varphi(rc, n) = \varphi(c, rn) = r\varphi(c, n)$. Define $\psi : B \times N \to P$ by $\psi(b, n) = \varphi(\beta(b), n)$. Then ψ is bilinear. Thus, there exists a unique $\tilde{\psi} : B \otimes_R N \to P$ an R-module homomorphism. We now show that $\alpha \otimes 1(A \otimes N) \subseteq \ker \tilde{\psi}$. $\tilde{\psi}(\alpha \otimes 1(a \otimes n)) = \tilde{\psi}(\alpha(a) \otimes n) = \varphi(\beta \circ \alpha(a), n) = \varphi(0, n) = 0$.

Thus, we get a unique induced R-mod homomorphism $\bar{\psi} : B \otimes_R N/\alpha \otimes 1(A \otimes_R N) \to P$ so by the universal property, $B \otimes_R N/\alpha \otimes 1(A \otimes_R N) \simeq C \otimes_R N$.

Warning: Tensor is not always left exact! $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2 \to 0$, tensor with $\mathbb{Z}/2$, and get $\mathbb{Z} \otimes \mathbb{Z}_2 \to \mathbb{Z} \otimes \mathbb{Z}/2 \to \mathbb{Z}/2 \otimes \mathbb{Z}/2 \to 0$ Specifically, $\mathbb{Z} \otimes \mathbb{Z}/2 \simeq \mathbb{Z}/2$, but the map given by multiplication by 2 is the zero map, so it is not injective.

Definition 2.3 (Flat Module)**.** *An R-module M is flat iff $- \otimes_R M$ is exact. That is, if $P \to P'$ is an injection, so is $P \otimes M \to P' \otimes M$.*

<u>Localization</u>

Motivation: We put the Zariski Topology on k^n, the closed sets are of the form $V(I)$ for some I. We ask: what are the rational functions defined everywhere on $k^n \setminus V(f)$? Well, they're of the form p/f^i where $p \in S$, $i \geq 0$, that is, elements of $S[f^{-1}]$.

Definition 2.4 (Localization)**.** *Let $U \subset R$ be a multiplicatively closed set ($u, u' \in U \Rightarrow uu' \in U$, $1 \in U$).*

For an R-module M, we set $M[U^{-1}] = \{(m, u) : m \in M, u \in U\}/\sim$ where $(m, u) \sim (m', u')$ iff $\exists v \in U$ such that $v(u'm - um') = 0$. We write (m, u) as m/u.

If $M = R$, then $R[U^{-1}]$ is a ring, with $(r/u)(r'/u') = rr'/uu'$.

Example: $R = M = \mathbb{Z}$, $U = \mathbb{Z} \setminus \{0\}$, then $R[U^{-1}] = \mathbb{Q}$.

Check: If M is an R-module, then $M[U^{-1}]$ is also an R-module by $r(m, u) = (rm, u)$ and $(m, u) + (m', u') = (u'm + um', uu')$.

Example: If R is a domain, then $U = R \setminus \{0\}$ gives $R[U^{-1}]$ is the field of fractions, or quotient ring, of R. In general, let $U = \{\text{nonzero divisors in } R\}$, then $K(R) = R[U^{-1}]$ is the total quotient ring of R.

Example: $R = k[x]$, $U = \{x^i : i \geq 0\}$, then $R[U^{-1}] = k[x, x^{-1}]$ is the ring of Laurent Polynomials.

Warning: The localization of a nonzero module can be zero!

Example: $R = \mathbb{Z}$, $M = \mathbb{Z}/5$. Let $U = \{5^i : i \geq 0\}$. $M[U^{-1}] = 0$ as $(m, u) \sim (0, 1)$ for all $m \in \mathbb{Z}/5$ as $5(1m - u0) = 0$.

Proposition 2.3. *Let U be a multiplicatively closed set of R and M an R-module, let $\varphi : M \to M[U^{-1}]$ be an R-module homomorphism $\varphi(m) = m/1$.*

Then $\varphi(m) = 0$ iff there is $u \in U$ with $um = 0$, and if M is a finitely generated R-module, then $M[U^{-1}]$ is zero iff there is a $u \in U$ that annihilates M.

Proof. $m/1 = 0/1$ iff $\exists u \in U$ with $u(1m - u0) = um = 0$.

Suppose M is finitely generated by $\{m_1, \ldots, m_s\}$. If there exists $u \in U$ such that $um = 0$ for all $m \in M$, then $m/u' = 0/1$ for all $m/u' \in M[U^{-1}]$. Conversely, suppose that $M[U^{-1}] = 0$, then $m_i/1 = 0$ for all i, so there exists u_i such that $u_i m_i = 0$ for each i, let $u = \prod u_i$. Then $uM = 0$. □

Notation: For any $U \subset R$, we'll denote by $R[U^{-1}]$ the localization $R[\tilde{U}^{-1}]$ where $\tilde{U}$ is the multiplicative closure of U.

The most important example is if P is a prime ideal of R and $U = R \setminus P$.

Notation: $R[(R \setminus P)^{-1}] = R_P$, and $M[(R \setminus P)^{-1}]_P$.

The residue class field $\kappa(P) = R_P/P_P$, where P_P is $\varphi(P)R_P$.

If $R = \mathbb{Z}$, then $\mathbb{Z}_0 = \mathbb{Q}$, $\kappa(0) = \mathbb{Q}$. $P = (p)$, so $\mathbb{Z}_P = \{a/b : p \not| b\}$, and $P_P = \{a/b : p|a, p \not| b\}$. Then $\kappa(P) = \mathbb{Z}_P/P_P \simeq \mathbb{Z}/P$.

R_P is an example of a local ring.

Definition 2.5 (Local Ring)**.** *A ring R is local if it has a unique maximal ideal.*

Proposition 2.4. *Let $\varphi : R \to R[U^{-1}]$ be the map $r \mapsto r/1$.*

For any ideal $I \subseteq R[U^{-1}]$, we have $I = \varphi^{-1}(I)R[U^{-1}]$. Thus that map $I \mapsto \varphi^{-1}(I)$ is an injection on the set of ideals in $R[U^{-1}]$ to the set of ideals of R. This preserves inclusions and intersections, and takes primes to primes.

An ideal J is of the form $\varphi^{-1}(I)$ for some ideal $I \subset R[U^{-1}]$ iff $J = \varphi^{-1}(JR[U^{-1}])$ iff for $u \in U$, $ur \in J \Rightarrow r \in J$ for $r \in R$. In particular, $I \mapsto \varphi^{-1}(I)$ gives a bijection between the primes in $R[U^{-1}]$ and the primes of R not meeting U.

Proof. $I \mapsto \varphi^{-1}(I)$ gives an injection $\{\text{primes of } R[U^{-1}]\} \to \{\text{primes of } R\}$. Suppose that J is $\varphi^{-1}(I)$. Then $ur \in J$ implies $r \in J$ for $u \in U$, $r \in R$, so $J \cap U = \emptyset$, as otherwise $u \in J \cap U$, then $u1 \in J$, so $1 \in J$, so $J = R$. □

Corollary 2.5. *R_P is a local ring.*

Note: If $\varphi : R \to S$ is a ring homomorphism with $\varphi(u)$ a unit of S for all $u \in U$, then if $v(u'r - r'u) = 0$, $\varphi(v(u'r - ur')) = 0$, $\varphi(v)(\varphi(u')\varphi(r) - \varphi(u)\varphi(r')) = 0$.

Since $\varphi(u)$ is a unit, $\varphi(u')\varphi(r) - \varphi(u)\varphi(r') = 0$ can be written as $\varphi(r)\varphi(u)^{-1} = \varphi(r')\varphi(u')^{-1}$. So we can define $\tilde{\varphi} : R[U^{-1}] \to S$ by $\tilde{\varphi}(r/u) = \varphi(r)\varphi(u)^{-1}$.

In fact, we have a universal property of localization: If $\varphi : R \to S$ is a ring homomorphism with $\varphi(u)$ a unit for all $u \in U$, then $\exists! \tilde{\varphi}$ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr] & S \\ & R[U^{-1}] \arrow[u, "\exists!\tilde{\varphi}"'] \end{tikzcd}$$

If $\varphi : M \to N$ is an R-module homomorphism, then $\tilde{\varphi} : M[U^{-1}] \to N[U^{-1}]$ defined by $\tilde{\varphi}(m/n) = \varphi(m)/u$ is an $R[U^{-1}]$ homomorphism.

Check well defined: $m/u = m'/u'$ implies $\exists v$ with $v(mu' - um') = 0$, so $v(u'\varphi(m) - u\varphi(m')) = 0$.

Lemma 2.6. *The map of R-modules $\alpha : R[U^{-1}] \otimes_R M \to M[U^{-1}]$ by $\alpha(r/u \otimes m) = rm/u$ is an isomorphism.*

Proof. We must first check that α is well defined. Define $\tilde{\alpha} : R[U^{-1}] \times M \to M[U^{-1}]$ by $(r/u, m) \mapsto rm/u$. This is bilinear and $\tilde{\alpha}(rs/u, m) = \tilde{\alpha}(r/u, sm) = rsm/u$, so we get a map on the tensor product.

Now define and inverse map $\beta : M[U^{-1}] \to R[U^{-1}] \otimes_R M$ by $m/u \mapsto 1/u \otimes_R m$. This is well defined, as $m'/u' = m/u$ means that for some $v \in U$, $v(um' - u'm) = 0$, so $\beta(m/u) = \frac{1}{u} \otimes_R m = vu'/vuu' \otimes_R m = \frac{1}{vuu'} \otimes_R vu'm = \beta(m'/u')$.

Check that it is an R-module homomorphism.

Finally, check that $\beta = \alpha^{-1}$. $\beta \circ \alpha(r/u \otimes m) = \beta(rm/u) = 1/u \otimes rm = r/u \otimes m$.

$\alpha \circ \beta(m/u) = \alpha(1/u \otimes m) = m/u$. □

Lemma 2.7. *$R[U^{-1}]$ is a flat R-module.*

Proof. Suppose that $0 \to A \xrightarrow{\alpha} B \to C \to 0$ is exact. It is enough to show that $A \otimes R[U^{-1}] \xrightarrow{\alpha \otimes 1} B \otimes R[U^{-1}]$ is injective. These are isomorphic, by the previous lemma, to $A[U^{-1}] \to B[U^{-1}]$ with $\tilde{\alpha}(a/u) = \alpha(a)/u$ is injective.

Suppose $\tilde{\alpha}(a/u) = 0$ so there exists $v \in U$ with $v\tilde{\alpha}(a/u) = 0$, $v\alpha(a)/u) = 0$ in $B[U^{-1}]$, so there is $v \in U$ with $v'(v\alpha(a) - u0) = 0$, so $v'v(\alpha(a)) = 0$, so $\alpha(v'va) = 0$, α is injective, so $v'va = 0$, so a/u is 0 in A. □

Exercise: $M_1, M_2 \subseteq M$ are R-modules, show that $(M_1 \cap M_2)[U^{-1}] = M_1[U^{-1}] \cap M_2[U^{-1}]$.

Hint: $0 \to M_1 \cap M_2 \to M \to M/M_1 \oplus M/M_2$ is exact.

Next: True Locally often implies True Globally

Lemma 2.8. *Let R be a ring, M an R-module*

1. *If $m \in M$ then $m = 0$ if and only if $, /1 = 0$ in each localization of M at a maximal prime $\mathfrak{m}$ of R.*

2. *$M = 0$ iff $M_{\mathfrak{m}} = 0$ for each maximal ideal $\mathfrak{m}$ of R.*

Proof. $m/1$ is zero in $M_{\mathfrak{m}}$ if any only if $\exists u \notin \mathfrak{m}$ with $um = 0$. ie, the annihilator of m in M, $I = \{r \in R : rm = 0\}$ is not contained in $\mathfrak{m}$. So if $m/1 = 0$ in every localization of M at a maximal prime, then I is not contained in any maximal ideal of R, which is a contradiction, so $m = 0$. $\square$

Corollary 2.9. *Let $\alpha : M \to N$ be an R-module homomorphism. Then α is injective, surjective or isomorphism iff $\alpha_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective, surjective or isomorphism for all maximal ideals $\mathfrak{m}$ of R.*

Proof. We have $0 \to \ker\alpha \to M \xrightarrow{\alpha} N \xrightarrow{s} \operatorname{coker}\alpha \to 0$. So $0 \to \ker(\alpha)_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}} \to \operatorname{coker}(\alpha)_{\mathfrak{m}} \to 0$ so if $\alpha_{\mathfrak{m}}$ is injective for all $\mathfrak{m}$, then $\ker(\alpha)_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$ so $\ker\alpha = 0$, similarly for $\operatorname{coker}\alpha$. $\square$

Next: (S is an R-algebra) $S \otimes_R \hom(M, N) \to \hom_S(S \otimes_R M, S \otimes_R N)$ by $s \otimes_R \varphi \mapsto s \otimes \varphi = s(1 \otimes \varphi)$. Check that this is well-defined.

Define $\tilde{\alpha} : S \times \hom_R(M, N) \to \hom_S(-, -)$ by $\tilde{\alpha}(\varphi) = s(1 \otimes \varphi) \in \hom_S(S \otimes_R M, S \otimes_R N)$ is bilinear and respects the R-action, so α is well defined. We'll see that it is an isomorphism if S is a flat R-module and M is finitely presented.

Recall: M is finitely generated iff $\exists \alpha$ such that $R^2 \xrightarrow{\alpha} M \to 0$ is exact. It finitely presented if $\ker\alpha$ is also finitely generated.

Fact: If R is Nötherian then finitely generated implies finitely presented.

A corollary of this is that if M is finitely presented, then $\hom_R(M, N)$ localizes, that is, $\hom_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}]) \simeq \hom_R(M, N)[U^{-1}]$.

Lemma 2.10. *If R is Nötherian and M is finitely generated, then every submodule of M is finitely generated. Thus, every finitely generated module is finitely presented.*

Proof. If M is f.g., then $\exists\, R^s \xrightarrow{\varphi} M \to 0$, and $\ker\varphi$ is a submodule of the finitely generated R-module R^s, so the second sentence follows from the first.

Now suppose that N is a submodule of M, where M is gen by $m_1, \ldots, m_s$. The proof is by induction on s. If $s = 1$, then $M \simeq Rm_1$, we let $I = \ker(R \to M)$, so $M \simeq R/I$. Thus, $\varphi^{-1}(N)$ is an ideal in R, so $\varphi^{-1}(N)$ is finitely generated by $n_1, \ldots, n_k$, since R is Nötherian, so $\varphi(n_1), \ldots, \varphi(n_k)$ generate N.

Now suppose that the lemma holds for all $s' < s$. Consider $\tilde{N} \subseteq M/Rm_1$ is generated by $m_2, \ldots, m_s$, so by induction $\tilde{N}$ is generated by $\{\bar{g}_1, \ldots, \bar{g}_\ell : g_i \in N, 1 \le i \le \ell\}$. Also, $N \cap Rm_1$ is finitely generated by $h_1, \ldots, h_r$. So for $n \in N$, $\bar{n} = \sum r_i \bar{g}_i$ and $n - \sum r_i g_i \in N \cap Rm_1$, so $n - \sum r_i g_i = \sum r_j h_j$ so $g_1, \ldots, g_\ell, h_1, \ldots, h_r$ generate N. $\square$

This is NOT true if R is not Nötherian. eg $R = k[x_1, x_2, \ldots]$, $M = R$, $N = (x_1, \ldots, x_n, \ldots)$ is an infinitely generated submodule of M.

Next: Move towards localization of hom.

Proof. We first prove the proper when $M = R$. $\alpha_R : S \otimes_R \hom_R(R, N) \to \hom_S(S \otimes_R R, S \otimes_R N)$ by $s \otimes \varphi \mapsto s(1 \otimes \varphi)$.

$S \otimes \varphi(1) \to s((1 \otimes \varphi)(1 \otimes 1)) = s \otimes \varphi(1)$.

Similarly, if $M = R^s$, then $\alpha_{R^s} : S \otimes_R N^s \to (S \otimes N)^s$, so finally, we take M finitely presented.

As such, we have $R^\ell \to R^s \to M \to 0$. We write $-'$ for $S \otimes -$, and so we apply this and get $(R^\ell)' \to (R^s)' \to M' \to 0$, we apply $\hom_R(-, N)$ and then $S \otimes -$, and we get the correct diagram and apply the five lemma. $\square$

3 Primary Decomposition

Consider $V(xy) \subseteq \mathbb{C}^2$. Then $V(xy) = V(x) \cup V(y)$, so we can break it into irreducible varieties.

Proposition 3.1. *A variety $V(I) \subseteq k^n$ can be written uniquely as $V_1 \cup \ldots \cup V_k$ where V_i are irreducible subvarieties and no $V_i \subset V_j$ for $i \neq j$.*

Proof. We first show that such a decomposition exists. Let $\mathscr{S}$ be the set of all varieties V that do not have such a decomposition into irreducibles. Since $k[x_1, \ldots, x_n]$ is Nötherian, $\mathscr{S}$ has a minimal element, $V(I)$. Since $V(I)$ is in $\mathscr{S}$, it is not irreducible, so we can write $V(I) = V_1 \cup V_2$ for V_1, V_2 proper subvarieties. One of these must not have an irreducible decomposition, else $V(I)$ would, but this contradicts minimality of $V(I)$

For uniqueness, suppose that $V(I) = V_1 \cup \ldots \cup V_k = V_1' \cup \ldots \cup V_\ell'$. So $V_1' = V_1' \cap V(I) = (V_1' \cap V_1) \cup \ldots \cup (V_1' \cap V_k)$. V_1' is irreducible, and each of these is a subvariety of V_1', so as V_1' is irreducible, we must have some V_i such that $V_1' \cap V_i = V_1'$ so $V_1' \subseteq V_i$. Then $V_i = (V_1' \cap V_i) \cup (V_2' \cap V_i) \cup \ldots \cup (V_\ell' \cap V_i)$, so there is a j such that $V_i = V_j' \cap V_i$, so $V_i \subseteq V_j'$, so $V_1' \subseteq V_i \subseteq V_j'$, so $j = 1$. Consider $Z = V_2' \cup \ldots V_\ell' = V_1 \cup \ldots \cup \hat{V}_i \cup \ldots \cup V_k = \overline{V(I) \setminus V_1'}$, and then induction. $\square$

Note: If $I = \sqrt{I}$ and $V(I)$ is irreducible, I is prime.

Definition 3.1 (Associated Prime)**.** *Let R be a ring and M an R-module. A prime P of R is associated to M if it is the annihilator of an element of M. We write $\mathrm{Ass}_R(M)$ for the set of all associated primes of M as an R-module.*

Notation: If $I \subseteq R$ is an ideal, write $\mathrm{Ass}_R(I)$ for $\mathrm{Ass}_R(R/I)$. We can get away with this, because $\mathrm{Ass}_R(I)$ is rarely interesting, eg, if R is a domain, then $\mathrm{Ass}_R(M) = \{(0)\}$ for $M = I$.

eg, if P is prime, $\mathrm{Ass}_R(P) = \{P\}$.

eg, if $V = V_1 \cup \ldots \cup V_k$, is the irreducible decomposition of a variety V, then $I(V_i)$ will be the associated primes of $I(V)$.

eg, $R = \mathbb{Z}$, $\mathrm{Ass}_\mathbb{Z}(n) = \mathrm{Ass}_\mathbb{Z}(\mathbb{Z}_n) =$set of prime factors

Lemma 3.2. *If R is Nötherian then $R[U^{-1}]$ is Nötherian.*

Proof. Let I be an ideal in R. Then $I = \varphi^{-1}(I)R[U^{-1}]$ where $\varphi : R \to R[U^{-1}]$ has $\varphi(r) = r/1$. Then $\varphi^{-1}(I)$ is an ideal of R, so finitely generated and, φ of those generators must generate I. $\square$

This shows that "Nötherian" is "better" than "finitely generated over a field", ie, quotient of a polynomial ring.

Lemma 3.3 (Prime Avoidance)**.** *Suppose that $I_1, \ldots, I_n, J$ are ideals of R and $J \subseteq \cup_{j=1}^n I_j$. If R contains an infinite field, or if all but two of the I_j are prime, then J is contained in one of the I_j. If R is $\mathbb{Z}$-graded and J is generated by homogeneous elements of* $\deg > 0$*, and all the I_j are prime, then it is enough to assume that all homogeneous elements of J are contained in $\cup_j I_j$.*

Proof. If R contains an infinite field k, then J is a k-vector space, also each $J \cap I_j$ is a k-vector subspace. If $J \not\subseteq I_j$ for all j, then $J \cap I_j$ is a proper subspace of J, but $J = \cup_{j=1}^n J \cap I_j$, and we cannot write a vector space over an infinite field as a finite union of proper subspaces. If one $I_j \subseteq J$, then quotient by it and repeat.

Now consider a general R, but all but two of the I_j are prime. The proof is by induction on n. If $n = 1$, then $J \subseteq I_1$.

If $n = 2$, $J \subseteq I_1 \cup I_2$, if $J \not\subset I_1$, $J \not\subset I_2$ we can find $x_1 \in J \cap I_1 \setminus I_2$ and $x_2 \in J \cap I_2 \setminus I_1$. But then $x_1 + x_2 \in J_1$, so $x_1 + x_2 \in I_1 \cup I_2$, but $x_1 + x_2 \notin I_1, I_2$, a contradiction.

Suppose $n > 2$. $J \subseteq \cup I_j$, $J \not\subset I_j$. So again we take $x_i \in J \cap I_i \setminus \cup_{i \neq j} I_j$. After reordering, we may assume that I_1 is prime. Consider $f = x_1 + \prod_{j=2}^n x_j \in J$. $x_1 \in I_1 \setminus \cup_{j=2}^n I_j$, the product is in $\cap_{j=2}^n I_j \setminus I_1$, since I_1 is prime. So $f \in \cup I_i$ but $f \notin I_j$ for any j, a contradiction.

Finally, assume R is graded. The Proof is almost the same. In the $n = 2$ case, we need to consider $x_1^k + x_2^\ell$ for some k, ℓ to make $x_1^k + x_2^\ell$ homogeneous. □

Proposition 3.4. *Let R be a ring and M an R-module. If I is maximal among all ideals of R that are annihilators of elements of M then I is prime and so belongs to* $\mathrm{Ass}_R(M)$*. Thus, if R is Nötherian,* $\mathrm{Ass}_R M$ *is nonempty and* $\cup_{P \in \mathrm{Ass}_R M} P = 0 \cup \{$*zero divisors of M*$\}$*. (that is, $r \in R$ nonzero such that $\exists m \neq 0$ with $rm = 0$)*

Proof. Let P be such an ideal maximal with respect to the property of annihilating an element of M. Let $rs \in P$ for $r, s \in R$. Let $m \in M$ have $P = \mathrm{Ann}_R(m)$. Then if $sm = 0$, we have $s \in P$. Otherwise $(rs)m = r(sm) = 0$ so $r \in \mathrm{Ann}_R(sm)$. But also if $p \in P$, $psm = s(pm) = 0$, so $r + P \subseteq \mathrm{Ann}_R(sm)$. Since $sm \neq 0$, $\mathrm{Ann}_R(sm) \neq R$, so $\mathrm{Ann}_R(sm) = P$. So $r \in P$. This shows that P is prime. We now check that $\cup_{P \in \mathrm{Ass}_R(M)} P = 0 \cup \{\text{zero divs}\}$. If $0 \neq p \in P \in \mathrm{Ass}_R(M)$, then $\exists m \in M$ with $pm = 0$, so p is a zero divisor on M. This shows $\subseteq$. Conversely, if $r \neq 0$ is a zero divisor, then $\exists m \in M$ with $rm = 0$, so $r \in \mathrm{Ann}_R M$. Let P be an ideal containing $\mathrm{Ann}_R M$ that is maximal with respect to annihilating some element of M. Then P is prime so $P \in \mathrm{Ass}_R M$, so $r \in \cup P$. □

Corollary 3.5. *Suppose that M is a module over a Nötherian ring R.*

1. *If $m \in M$, then $m = 0$ iff $m/1 = 0 \in M_P$ for all maximal associated primes of M.*

2. *If K is a submodule of M, then $K = 0$ iff $K_P = 0$ for all maximal $P \in \operatorname{Ass} M$.*

3. *If $\varphi : M \to N$ is an R-module homomorphism, then φ is an injective iff $\varphi_p : M_p \to N_p$ is an injection for each $P \in \operatorname{Ass} M$.*

Proof. If $0 \neq m \in M$, then $\exists P \in \operatorname{Ass} M$ containing $\operatorname{Ann} m$. Then some $P \cap \operatorname{Ann} m = \{0\}$, we get $m/1 \neq 0$ in M_P. If $\operatorname{Ann} M = 0$, then any P works. We take P maximal to get the result. Part 1 implies 2 and 2 implies 3. □

Q: How can we find ALL associated primes?

Lemma 3.6. *If R is a Nötherian ring and M is a finitely generated R-module, then M has a filtration $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$ with $M_{i+1}/M_i \simeq R/P_i$ for some prime P_i of R.*

Proof. If $M \neq 0$ then there is an associated prime $P_1 \in \operatorname{Ann}(m_1)$ for $m_1 \in M$. Set $M_1 = Rm_1 \simeq R/P_1$. If $M_1 \neq M$, consider M/M_1. This has an associated prime $P_2 = \operatorname{Ann}(\bar{m}_2)$, set $M_2 = M_1 + Rm_2$. By construction, $M_2/M_1 \simeq R/P_2$. Continue in this fashion, this must terminate with some $M_i = M$, else we would have an infinite ascending chain of submodules of M. This is impossible as M is finitely generated over a Nötherian ring. □

Lemma 3.7. *M is an R-module.*

1. *If $M = M' \oplus M''$, then $\operatorname{Ass}_R(M) = \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'')$*

2. *If $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ is a s.e.s. of R-modules, then $\operatorname{Ass}_R(M') \subseteq \operatorname{Ass}_R(M) \subseteq \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'')$.*

Proof. 1. Follows from 2.

2. Suppose $m \in M'$ with $\operatorname{Ann}_R(m) = P$ prime. Then $\operatorname{Ann}_R(i(m)) = P$, so $O \in \operatorname{Ass}_R(M)$.

   Now suppose $P \in \operatorname{Ass}_R(M) \setminus_R (M')$. $P = \operatorname{Ann}_R(m)$ for $m \in M$. So $Rm \simeq R/P$. Now for all $r \in R$ with $rm \neq 0$, we have $\operatorname{Ann}_R(rm) = P$, since $s \in P \Rightarrow srm = 0$ and if $srm = 0$ then $sr \in P$, and $r \notin P$(since $rm \neq 0$) so $s \in P$. This means that $Rm \cap i(M') = \{0\}$.

   We now claim that $\operatorname{Ann}_R(p(m)) = P$ since $Rp(m) = p(Rm) \simeq Rm = R/P$, so $P \in \operatorname{Ass}_R(M'')$.

□

Corollary 3.8. *If R is Nötherian, M finitely generated, and $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$ with $M_i/M_{i-1} \simeq R/P_i$, then $\operatorname{Ass}_R(M) \subseteq \{P_1, \ldots, P_n\}$, so $\operatorname{Ass}_R(M)$ is a finite nonempty set.*

Proof. When $n = 1$, $M = R/P_1$, which has $\mathrm{Ass}_R(R/P_1) = \{P_1\}$.

For $n > 1$, $0 \to M_1 \to M \to M/M_1 \to 0$ is ses, both ends have filtrations, the first $0 \subsetneq M_1$, the second $0 \subsetneq M_2/M_1 \subsetneq M_3/M_1 \subsetneq \ldots \subsetneq M/M_1$. By induction, $\mathrm{Ass}_R(M_1) \subseteq \{P_1\}$, and $\mathrm{Ass}_R(M/M_1) \subseteq \{P_2, \ldots, P_n\}$, so $\mathrm{Ass}_R(M) \subseteq \{P_1, \ldots, P_n\}$. □

eg, $k[x,y]/(x^2y, xy^2)$ has $0 \subsetneq Ry^2/(x^2y, xy^2) \subsetneq R\{x^2, y^2\}/(x^2y, xy^2) \subsetneq R\{xy, x^2, y^2\}/(xy^2, x^2y) \subsetneq M$.

Now $Ry^2/(x^2y, xy^2) = R/(x)$ and $R\{x^2, y^2\}/(xy^2, x^2y)/Ry^2/(xy^2, x^2y) = Rx^2/(x^2y, xy^2) \simeq R/(x)$ and $M_3/M_2 \simeq R/(x,y)$. Set $M_4 = R\{x, y^2\}/(xy^2, x^2y)$, $M_4/M_3 \simeq R/(x,y)$. Set $M_5 = R\{x,y\}/(x^2y, xy^2)$, $M_5/M_4 \simeq R/(x,y)$, and $M = R\{1\}/(x^2y, xy^2)$ and $M/M_5 \simeq R/(x,y)$. So we now have a filtration $0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq M_4 \subsetneq M_5 \subsetneq M$, so $P_1 = (x)$, $P_2 = (y)$, $P_3 = P_4 = P_5 = (x,y)$.

Warning: There is not always a filtration with all P_i associated! e.g. $R = k[x,y,z,w]$, $I = (x,y) \cap (z,w) = (xz, xw, yz, yw)$.

Claim: $\mathrm{Ass}_R(I) = \{(x,y), (z,w)\}$. Claim 2: There is no filtration $0 \subsetneq M_1 \subsetneq M$ with $M_1 \simeq R/(x,y)$, $M/M_1 \simeq R/(z,w)$.

Theorem 3.9. *R Nötherian, M is finitely generated.*

1. *Associated primes commutes with localization, ie* $\mathrm{Ass}_{R[U^{-1}]}(M[U^{-1}]) = \{PR[U^{-1}] | P \in \mathrm{Ass}_R(M)$ *with* $P \cap U = \emptyset\}$
2. $\mathrm{Ass}_R(M)$ *contains all primes minimal over* $\mathrm{Ann}_R(M)$.

Proof. If $P \in \mathrm{Ass}_R(M)$, then there exists $m \in M$ with $P = \mathrm{Ann}_R(m)$. So $Rm \simeq R/P$, and we get an inclusion $R/P \to M$. As localization is exact, $(R/P)[U^{-1}] \to M[U^{-1}]$ is an inclusion, so if $P \cap U = \emptyset$, $PR[U^{-1}]$ is prime in $R[U^{-1}]$, then $PR[U^{-1}] \in \mathrm{Ass}_{R[U^{-1}]}(M[U^{-1}])$.

Conversely, suppose that $Q \in \mathrm{Ass}_{R[U^{-1}]}(M[U^{-1}])$, then $Q = PR[U^{-1}]$ for some prime P of R with $P \cap U = \emptyset$. Since R is Nötherian, we know that $R[U^{-1}]$ is, so $PR[U^{-1}]$ is finitely generated. Thus, $R[U^{-1}]/PR[U^{-1}]$ is finitely presented. Thus, $\hom_{R[U^{-1}]}(R[U^{-1}]/PR[U^{-1}], M[U^{-1}]) \simeq \hom_R(R/P, M)[U^{-1}]$, thus the inclusion $\varphi : R[U^{-1}]/Q \to M[U^{-1}]$ must be f/u for some $g \in \hom_R(R/P, M)$ since φ is injective, so is f, and so $R/P \to M$ is an injection, so $P \in \mathrm{Ass}_R(M)$.

For part 2, we consider the R_P module M_P with P a minimal prime over $\mathrm{Ann}_R(m)$. $\mathrm{Ass}_{R_P}(M_P) \neq \emptyset$ and if $Q \in \mathrm{Ass}_{R_P}(M_P)$, then $P'_P = Q \subsetneq P_P$, but if $P'_P \subsetneq P_P$ then $P' \not\supseteq \mathrm{Ann}_R(M)$, so there is $r \in \mathrm{Ann}_R(M)$ with $r \notin P'$ so that $r/1 \notin P'_P$ and $r/1 \in \mathrm{Ann}_{R_P}(M_P)$. Thus, $\mathrm{Ann}_{R_P}(M_P) \not\subseteq P'_P$, so P'_P is not associated.

This means that $\mathrm{Ass}_{R_P}(M_P) = \{P_P\}$, so $P \in \mathrm{Ass}_R(M)$. □

Fact: If I is radical then $I = \cap P$ for P a prime containing I or for P primes minimal wrt containing I.

Lemma 3.10. *If R is commutative, U is multiplicatively closed and I is maximal among ideals not meeting U, then I is prime.*

Proof. Suppose that $fg \in I$. If $f, g \notin I$, then $I + (f) \cap U \neq \emptyset, I + (g) \cap U \neq \emptyset$, so there exists $i, i' \in I$, $r, r' \in R$ with $i + rf, i' + r'g \in U$ so $(i + rf)(r' + r'g) \in U$, is equal to $ii' + ir'g + rf'i + rr'fg \in I$, contradicting that $I \cap U = \emptyset$.

So either $f \in I$ or $\in I$, so I is prime. □

Corollary 3.11. *$I \subseteq R$ is an ideal, then $\sqrt{I} = \cap P$ over primes containing I. In particular, the intersection of all primes is $\sqrt{0}$, the set of nilpotents.*

Proof. $\sqrt{I} \subseteq \cap P$ is straightforward.

Suppose that $f \in \cap P \setminus \sqrt{I}$. $U = \{f^i : i \geq 0\}$, then $\sqrt{I} \cap U = \emptyset$. Let J be an ideal containing $\sqrt{I}$ max wrt $J \cap U = \emptyset$, then J is prime which contains I, so $f \in J$, contradiction, so $\cap P = \sqrt{I}$. □

Corollary 3.12. *If $I = \sqrt{I}$, then $I = \cap P$, P minimal over I, and $\mathrm{Ass}_R(I) = \{P | P$ is minimal over $I\}$.*

Next time, $I = \cap Q_i$, $\sqrt{Q_i} \in \mathrm{Ass}_R(I)$.

As $\sqrt{I} = \cap P$, P prime and $I \subseteq P$. So $\cap P$ over all primes are the nilpotent elements, and $\cap_{P \in \mathrm{Ass}} P = \sqrt{\mathrm{Ann}_R M}$.

First, IOUs.

1. If R is f.g. over a field, $R[U^{-1}]$ doesn't have to be. $k[x]_{(x)}$, for example. Suppose that $k[x]_{(x)}$ as a k-algebra by $f_1/g_1, \ldots, f_r/g_r$. Assume k is algebraically closed, look at the factors of the g_i. Only finitely many $x - \alpha$ show up, but k is infinite, so these cannot generate everything.

2. We looked at $= (x, y) \cap (z, w) = \cap P$. Suppose that $P_1 \cap P_2 = P_3 \cap P_4 \cap \ldots \cap P_n$ irredundant, all P_i necessary. So $P_1 \cap P_2 \subseteq P_3$, so $P_1 P_2 \subseteq P_3$, so $P_1 \subseteq P_3$ or $P_2 \subseteq P_3$, and so by irredundancy, $P_3 = P_1$ and $P_4 = P_2$.

Lemma 3.13. *If $I = \sqrt{I}$, then $\mathrm{Ass}(I) = \{P$ minimal over $I\}$.*

This is because $I = \cap P$ over the primes minimal over I.

In general, we replace primes by ideals with only one associated prime. $\mathrm{Ass}(R/P) = \{P\}$.

Definition 3.2 (P-primary)**.** *Let R be a Nötherian ring and M a finitely generated R-module.*

A submodule $N \subseteq M$ is P-primary if $\mathrm{Ass}_R(M/N) = \{P\}$.

Proposition 3.14. *Let P be a prime ideal in R. Then TFAE*

1. $\mathrm{Ass}_R(M) = \{P\}$

2. *P is minimal over $\mathrm{Ann}_R M$ and every element not in P is a non zero divisor on M.*

3. *A power of P annihilates M and every element not in P is a non zero divisor.*

Proof. $1 \Rightarrow 2$: If P is not minimal over $\operatorname{Ann}_R M$, then there exists P' minimal over $\operatorname{Ann}_R M$ with $\operatorname{Ann}_R M \subseteq P' \subsetneq P$. So $P' \in \operatorname{Ass}_R M$. Also, every zero divisor is in some associated prime, so they all lie in P.

$2 \Rightarrow 3$: Since elements outside of P are non zero divisors, we get $M \to M_P$ injective, so if a power of P_P annihilates M_P that power of P annihilates M. But P_P is minimal over $\operatorname{Ann}_{R_P} M_P$ and every prime is contained in P_P. So $\cap Q$ over $Q \in R_P$ prime, minimal over $\operatorname{Ann}_{R_P} M_P$, is equal to $P_P = \sqrt{\operatorname{Ann}_{R_P} M_P}$. Thus, $\exists k$ such that $P_P^k \subseteq \operatorname{Ann}_{R_P} M_P$.

$3 \Rightarrow 1$: Since $P^k \subseteq \operatorname{Ann}_R M \subseteq P$, and P must be contained in any prime containing $\operatorname{Ann}_R M$, so P is minimal over $\operatorname{Ann}_P M$, so $P \in \operatorname{Ass}_R M$. But also, every associated prime is contained in P, from the nonzero divisor assumption, so P is the only associated prime. □

Corollary 3.15. *Let I be an ideal in R. TFAE*

1. *I is P-primary*
2. *I contains a power of P and for all r, s with $rs \in I$ and $r \notin I$, we have $s \in P$*
3. *$\sqrt{I} = P$ and for all $r, s \in R$ with $rs \in I$, either $r \in I$ or there is a k such that $s^k \in I$.*

Proof. 1 and 2 are equivalent because they are 1 and 3 of the prop.

$2 \Rightarrow 3$: If $rs \in I$, $r \notin I$, then $s \in P$, so $\exists k$ with $s^k \in I$. Also, $P^k \subseteq I$ for some k, $P \subseteq \sqrt{I}$. If $f \in \sqrt{I} \setminus P$, then $\exists \ell$ such that $g = f^\ell \in I \setminus P$. But now $g \cdot 1 \in I$, $1 \notin I$ so $g \in P$, contradiction. Thus, $\sqrt{I} \subseteq P$.

$3 \Rightarrow 1$: Since $\sqrt{I} = P$, we know $P^k \subseteq I$ for some k, and if $rs \in I$, $r \notin I$, then $\exists \ell$ such that $s^\ell \in I$, so $s \in \sqrt{I} = P$. □

Theorem 3.16. *A proper submodule M' of M is the intersection of primary submodules.*

Definition 3.3 (Irreducible Submodule)**.** *A submodule N of M is irreducible if it cannot be written as the intersection $N = N_1 \cap N_2$ with $N \subsetneq N_1$ and $N \subsetneq N_2$.*

Lemma 3.17. *If M' is a proper submodule of M, then we can write $M' = \cap_{i=1}^k M_i$ where each M_i is irreducible.*

Proof. R Nötherian and M finitely generated implies that M is Nötherian.

So if the lemma is false, there exists a submodule N maximal with respect to not having an irreducible decomposition. In particular, N is not irreducible, so we write $N = N_1 \cap N_2$, with $N \subsetneq N_1$ and $N \subsetneq N_2$. But $N_1 = \cap_{i=1}^k M_i$ and $N_2 = \cap_{j=k+1}^\ell M_j$, so $N = \cap_{i=1}^\ell M_i$, contradiction. □

Lemma 3.18. *If $N \subseteq M$ is irreducible, then N is primary.*

Proof. Suppose $P \neq Q \in \operatorname{Ass}_R(M/N)$. Then $R/P \simeq R\bar{m}_1$ for some $\bar{m}_1 \in M/N$, and $R/Q \simeq R\bar{m}_2$ for some $\bar{m}_2 \in M/N$.

$R\bar{m}_1 \cap R\bar{m}_2 = \{0\}$, so $(N + m_1) \cap (N + m_2) = N$. □

Theorem 3.19. *Let M' be a proper submodule of M and write $M' = \cap M_i$ where M_i is P_i-primary. Then*

1. *Every associated prime of M/M' occurs among the P_i.*
2. *If the decomposition is irredundant, then the P_i are precisely the associated primes.*
3. *If the intersection is minimal, then each associated prime occurs exactly once, and if P is a minimal associated prime, then M_i is the P-primary component of M'.*

Proof. We first note that if $M' = \cap M_i$ with $\mathrm{Ass}_R(M/M_i) = \{P_i\}$, then $0 = \cap(M_i/M') \subseteq M/M'$ with $\mathrm{Ass}_R((M/M')/(M_i/M')) = \{P_i\}$. ie, we can replace M by M/M' and M' by 0, so we will assume that $M' = 0$.

1. So $0 = \cap M_i$, so $M \to \oplus M/M_i$ is an injection. So $\mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(\oplus M/M_i) = \cup \mathrm{Ass}_R(M/M_i) = \{P_1, \ldots, P_n\}$.
2. If the decomposition is irredundant, then $\cap_{i\neq j} M_i \neq 0$ for any j. So $\cap_{i\neq j} M_i = \cap_{i\neq j} M_i/(\cap_{i\neq j}(M_i \cap M_j)) \simeq (\cap_{i\neq j} M_i + M_j)/M_j \subseteq M/M_j$. So $\mathrm{Ass}_R(\cap_{i\neq j} M_i + M_j) \subseteq \mathrm{Ass}_R(M/M_j) = \{P_j\}$, so $\mathrm{Ass}_R(\cap_{i\neq j} M_i + M_j) = \{P_j\}$, so $O_j \in \mathrm{Ass}_R(M)$.
3. We first note that if $N_1, N_2 \subseteq M$ with $\mathrm{Ass}(M/N_i) = \{P\}$ for $i = 1, 2$, then $M/N_1 \cap N_2 \to M/N_1 \oplus M/N_2$ is an inclusion, so $\mathrm{Ass}(M/N_1 \cap N_2) \subseteq \mathrm{Ass}(M/N_1 \oplus M/N_2) = \{P\}$, so $\mathrm{Ass}(M/N_1 \cap N_2) = \{P\}$. Thus if $P_i = P_j$ we can replace M_i, M_j by $M_i \cap M_j$ to get a primary decomposition with fewer terms. So each P_i shows up at most once. But minimal implies irredundant, so each P_i shows up exactly once.

   Now suppose that P_i is minimal over $\mathrm{Ann}_R M$. We want to show that $M_i = \ker(M \to M_{P_i})$. Consider the diagram

$$\begin{tikzcd}
 & M_{P_i} \arrow[dr, "\gamma"] & \\
M \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & (M/M_i)_{P_i} \\
 & M/M_i \arrow[ur, "\delta"'] &
\end{tikzcd}$$

   We have $M_i = \ker \beta$. So show that $M_i = \ker \alpha$, it suffices to check that δ, γ are injections. δ is because $\mathrm{Ass}(M/M_i) = \{P_i\}$. Since $\cap M_j = 0$, $\phi : M \to \oplus M/M_j$ localizes to $\phi_{P_i} : M_{P_i} \to \oplus(M/M_j)_{P_i}$. γ is the ith component of ϕ_{P_i}. To see that γ is injective, it suffices to note that $(M/M_j)_{P_i} = 0$. If it weren't zero, we would have $\mathrm{Ass}_{R_{P_i}}((M/M_j)_{P_i}) = \{QR_{P_i} | Q \in \mathrm{Ass}_R(M/M_j) \text{ with } Q \cap (R \setminus P) = \emptyset\} = \{QR_{P_i} | Q = P_j \text{ and } Q \subseteq P_i\}$, which is empty as P_i is minimal.

$\square$

eg, $I = (x^2y^4, x^3y^3, x^4y^2) = (x^2) \cap (y^2) \cap (x^4, xy^4, y^7, x^3y^3) = (x^2) \cap (y^2) \cap (x^10, x^4y, x^3y^3, y^4)$

Proposition 3.20. *Let A be a finitely generated torsion free abelian group and let $R = \oplus_{a \in A} R_a$ and M be a graded R-module. If $P = \operatorname{Ann}_R M$ for any $m \in M$ and P is prime, then P is homogeneous and P is the annihilator of a homogeneous element.*

Proof. $A \simeq \mathbb{Z}^k$ for some k. Choose the isomorphism and $w \in \mathbb{R}^k$ sufficiently general and set $u \prec u'$ for $u, u' \in R^k$ if $w \cdot u < w \cdot u'$. (sufficiently general means that this is a total order).

Note that if $u < u'$ then $u + v < u' + v$. If P is not homogeneous, then there exists $f \in P$ and $a \in A$ with $f_a \notin P$ where $f = \sum_{a \in A} f_a$. We can assume in fact that no $f_a \in P$. Write $m = \sum m_a$. Then $0 = fm = f_1 m_1 + HOT$ where $\deg f_1 = \min\{a_i | f_{a_i} \neq 0\}$ and $\deg m_1 = \{a_i | m_{a_i} \neq 0\}$. So $f_1 m_1 = 0$. So if $m = m_1$ done. Otherwise, this is the base case of an induction on the number of nonzero components, b.

Suppose that it is true for small b. Write $f_1 m = \sum_{m_a \neq m_1} f_1 m_a$, this has fewer terms, so $P \subseteq I = \operatorname{Ann}_R f_1 m$. If $P = I$, then P is homogeneous by induction. Otherwise, there is $g \in I \setminus P$ with $g f_1 m = 0$ so $g f_1 \in P$ so $f_1 \in P$ as required. □

Lemma 3.21. *If M is a noetherian R-module and $M' \subseteq M$ with $M' = \cap M_i$ with M_i P_i-primary is minimal, let U be a multiplicatively closed set of R. Then $M'[U^{-1}] = \cap M_i[U^{-1}]$ over the submodules with $P_i \cap U = \emptyset$ is a minimal primary decomposition of $M'[U^{-1}]$ as an $R[U^{-1}]$-module.*

Proof. $M'[U^{-1}] = \cap M_i[U^{-1}]$, since localization commutes with intersection. If $P_i \cap U \neq \emptyset$, then $M_i[U^{-1}] = M[U^{-1}]$ since $(M/M_i)[U^{-1}]$ has no associated primes, it must be the zero module.

As $M'[U^{-1}] = \cap M_i[U^{-1}]$ with $P \cap U = \emptyset$, and $\operatorname{Ass}_{R[U^{-1}]}(M[U^{-1}]/M'[U^{-1}]) = \{PR[U^{-1}] |$ where $P \in \operatorname{Ass}_R(M/M')$ and $P \cap U = \emptyset\}$. So since $\cap M_i$ was minimal, each P_i was in $\operatorname{Ass}_R(M/M')$ and showed up exactly once, so in this new intersection. □

4 Integral Dependence

<u>Cayley-Hamilton Theorem</u>

In linear algebra, $p_A(X) = \det(A - xI)$

Cayley-Hamilton says $p_A(A) = 0$.

Slightly more abstractly, if V is an n-dimensional vector space over k, and $\varphi : V \to V$ is a linear map, then there exists $a_0, \ldots, a_{n-1} \in k$ such that $\varphi^n + \sum_{i=0}^{n-1} a_i \varphi^i = 0$.

Theorem 4.1. *Let R be a ring and M a finitely generated R-module that has a generating set with n elements. Let $\varphi : M \to M$ be an R-module homomorphism. If $\varphi(M) = IM$ for an ideal $I \subseteq R$, then there exists a monic polynomial*

$p(x) = x^n + p_1 x^{n-1} + \ldots + p_n$ with $p_j \in I^j$ for each j such that $p(\varphi) = 0$ as an endomorphism of M.

Proof. Let $m_1, \ldots, m_n$ be generators for M. Write $\varphi(m_j) = \sum_{i=1}^n a_{ij} m_i$. Let A be the matrix $A = (a_{ij})$ and $\underline{m} = (m_1, \ldots, m_n)^T \in M^n$. Regard M as an $R[x]$-module where $x \cdot m = \varphi(m)$.

Then $(Ix - A)m = 0$ for all $m \in M$, where $Ix : M \to M$ where if $m = \sum r_i m_i$, $Ix(m) = \sum r_i \varphi(m_i)$, then $Ix(m_i) = \varphi(m_i)$, and $Am_i = \sum_{j=1}^n a_{ji} m_j$. Let A' be the matrix of cofactors of $Ix - A$, recall from linear algebra that if $A = (a_{ij})$ then the cofactor matrix B is (b_{ij}) with $b_{ij} = (-1)^{i+j} \det(A^{ij})$.

Then $A'(Ix - A) = \det(Ix - A)I$, that is, $\det(Ix - A)m = 0$ for all $m \in M$, so $\det(Ix - A) \in R[x]$ and is in $\operatorname{Ann}_{R[x]} M$.

Let $p(x) = \det(Ix - A)$. $p(x)$ has degree n and $p(\varphi) = 0$ and if $p(X) = x^n + \sum_{i=0}^{n-1} p_i x^{n-i}$ then $p_i \in I^i$. □

More linear algebra: If $\varphi : V \to V$ is surjective, then V is injective, if V is a finite dimensional vector space.

Corollary 4.2. *Let R be a ring and let M be a finitely generated R-module.*

1. *If $\alpha : M \to M$ is a surjective R-module homomorphism, then α is an isomorphism.*
2. *If $M \simeq R^n$ then every set of n elements that generates M forms a free basis, in particular, the rank of M is well-defined.*

Proof.

1. Regard M as a module over $R[t]$ with t acting as α, so $tm = \alpha(m)$. Set $I = (t) \subseteq R[t]$, then $IM = M$ since α is surjective. Apply Cayley-Hamilton to the identity homomorphism, $1 : M \to M$ so there exists $x^n + p_1 x^{n-1} + \ldots + p_n$ with $p_i \in I^i$ and $(1 + p_1 1 + \ldots + p_n 1)m = 0$, so $(1 + p_1 + \ldots + p_n)m = 0$, write this as $1 - tq(t)$, so there exists $q(t) \in R[t]$ with $(1 - tq(t))m = 0$ for all $m \in M$. So $(1 - q(\alpha)\alpha)m = 0$, so $q(\alpha) \circ \alpha = 1$. Thus α is injective.

2. A set of n generators for M corresponds to a surjection $\beta : R^n \to M$. Since M is free of rank n, there exists $\gamma : M \to R^n$, then $\beta \circ \gamma : M \to M$ is surjective, and thus it is an isomorphism. So $\beta = (\beta\gamma) \circ \gamma^{-1}$ is an isomorphism, so that the given generators form a free basis.

   To finish we check that rank is well defined. 1) suppose that $R^m \simeq R^n$ for $m < n$, we extend our generating set of size m to one of size n by adding $n - m$ zeros. Then part 1 says that this is a free basis, but it contains zero, so it is a contradiction.

   A second proof is that we let P be a maximal ideal of R, then $R/P \otimes_R M \simeq (R/P)^m \simeq (R/P)^n$

□

Note: This is not true for injections! eg $\alpha : \mathbb{Z} \to \mathbb{Z}$ by $\alpha(x) = 2x$.

<u>Integral Dependence</u>

Definition 4.1 (Integral over R)**.** *Let S be an R-algebra and let $p(x)$ be a polynomial in $R[x]$. We say that $s \in S$ satisfies p if $p(s) = 0$. The element s is called integral over R if it satisfies some monic polynomial.*

The equation $p(s) = 0$ is the equation of integral dependence for s over R.

If every element of S is integral over R, we say S is integral over R.

eg $S = \mathbb{Q}(\sqrt{2})$ with $R = \mathbb{Z}$. $\sqrt{2}$ is integral over $\mathbb{Z}$, as it satisfies $x^2 - 2 = 0$. In fact, $a + b\sqrt{2}$ for any $a, b \in \mathbb{Z}$ is integral over $\mathbb{Z}$. $(x - a)^2 = 2b^2$.

Claim: These are all the elements integral over $\mathbb{Z}$. eg, $K = \mathbb{Q}(\sqrt{5})$, then $x = \frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$, as it satisfies $(2x-1)^2 = 5$ which is $4x^2-4x-4 = 0$, so $x^2 - x - 1 = 0$.

Definition 4.2 (Integral Closure)**.** *The collection of all elements of S integral over R is called the integral closure, or normalization, of R in S.*

Definition 4.3 (Number Field)**.** *A finite field extension of $\mathbb{Q}$ is called a number field. The integral closure of $\mathbb{Z}$ in a number field is called the ring of integers in that number field.*

Definition 4.4 (Normal)**.** *If R is a domain, then it's normalization is its integral closure in its field of fractions. If R is equal to its normalization, then we say that it is normal.*

eg, $\mathbb{Z}$ is normal, though proving this really proves the following:

Lemma 4.3. *Any UFD is normal.*

Proof. Consider r/s with r, s relatively prime. If $(r/s)^n + p_1(r/s)^{n-1} + \ldots + p_n = 0$, then $r^n + p_1 s p^{n-1} + \ldots + p_n s^n = 0$, which contradicts the relatively prime assumption. □

e.g. $k[x]$ is normal.

Theorem 4.4. *Let R be a ring and let $J \subseteq R[x]$ be an ideal. Let $S = R[x]/J$ and let s be the image of x in s.*

1. *S is generated by $\leq n$ elements as an R-module iff J contains a monic polynomial of deg $\leq n$. In this case, S is generated by $\{1, s, \ldots, s^{n-1}\}$. In particular, S is a finitely generated R-module iff J contains a monic polynomial.*

2. *S is a finitely generated free R-module iff J can be generated by a monic polynomial. Then S has a basis of the form $\{1, s, \ldots, s^{n-1}\}$.*

eg $\mathbb{Z}[x]/(2x + 1)$ is not finitely generated.

Proof. 1. The powers of x generated $R[x]$ as an R-module, and so generate S as well. So if J contains a monic polynomial, p, of degree n, then for $d \geq n$, we can write s^d in terms of smaller powers of s using $s^{d-n}p(s) = 0$, so $\{1, \ldots, s^{n-1}\}$ generate S. Conversely, suppose that S is generated by

$\leq n$ elements as an R-module. Multiplication by s is an endomorphism of S, so Cayley-Hamilton says that there exists a monic p of deg $\leq n$ with $p(s) = 0$, so $p(x) \in J$.

2. Suppose that J is generated by a monic polynomial p of degree n. Then from a, $\{1, \ldots, s^{n-1}\}$ generates S. if these do not form a free basis, then there are $a_i \in R$ with $\sum a_i s^i = 0$. Thus, $\sum a_i x^i \in J$ of degree $n-1$. This contradicts the fact that J is generated by p which has degree n. Thus, S is a free R-module with free basis $\{1, \ldots, s^{n-1}\}$. Conversely, we suppose that S is a free R-module of rank n. Then S is finitely generated, so by 1, J contains a monic p of degree n. Suppose there is $q \in J \setminus (p)$. Use the division algorithm to write $q = ap + r$ for $a, r \in R[x]$ with $\deg r < n$. Then $r \in J$, but if $r \neq 0$, then this would contradict $\{1, \ldots s^{n-1}\}$ being a free basis. So $r = 0$ and $q \in (p)$, thus $(p) = J$.

□

Definition 4.5 (Finite)**.** *An R-algebra S is finite over R if S is a finitely generated R-module.*

Corollary 4.5. *An R-algebra S is finite over R iff S is generated as an R-algebra by finitely many integral elements.*

Proof. If S is finite over R and $s \in S$, multiplication by s is an endomorphism of s. So Cayley-Hamilton shows that there exists monic p with coefficients in R and $p(s) = 0$, so s is integral over R¿

Thus, since S is a finitely generated R-algebra, it is generated by finitely many integral elements.

Conversely, suppose that S is generated by t integral elements as an R-algebra.

If $t = 1$, then $S \simeq R[x]/J$ for some J, and by the theorem, J contains a monic polynomial, so S is finite over R by the theorem.

We may assume that $t > 1$ and that the result is true for $t = 1$. Let S' be the subalgebra of S generated by the first $t-1$ generators of S. Then, by induction, S' is finite over R, so S' is generated, as an R-modules, by $\{s_1, \ldots, s_\ell\}$. The extra generator s for S is integral over R, so it is integral over S', so S is finite over S'. So S is generated as an S'-module by $t_1, \ldots, t_m$, but then $\{s_i t_j : 1 \leq i \leq \ell, 1 \leq j \leq m\}$ generates S as an R-module. So S is finite over R. □

Corollary 4.6. *If S is an R-algebra and $s \in S$, then s is integral over R iff there exists an S-module N and a f.g. R-submodule $M \subseteq N$ nor annihilated by any nonzero element of S such that $sM \subseteq M$.*

In particular, S is integral iff $R[s]$ is a finitely generated R-module.

Proof. If s is integral over R, take $N = S$, $M = R[s] \subset S$ is a finitely generated R-module and not annihilated by anything in S, since $s'1 = s' \neq 0$.

Conversely, if $\exists M \subseteq N$ with these properties, then multiplication by s is an R-module homomorphism. So by Cayley-Hamilton, there exists a monic p with coefficients in R such that $p(s)M = 0$, then $p(s) = 0$ in S, so S is integral over R. □

Theorem 4.7. *Let R be a ring and S be an R-algebra.. The set of all elements of S integral over R is a subalgebra of S.*

In particular, if S is generated by elements integral over R, then S is integral over R.

Proof. Let S' be the set of elements of S integral over R. We need to show that if $s, s' \in S'$ then ss' and $s + s'$ are in S'. Let $M = R[s]$, $M' = R[s']$, which are finitely generated R-module. Let $MM' = R\{fg, f \in M, g \in M'\}$, then MM' is a finitely generated R-module. $ss'MM' = (sM)(s'M') \subseteq MM'$, and $(s + s')MM' = (sM)M' + M(s'M')$, so by the corollary, since $MM' \subseteq S$ is a finitely generated submodule not annihilated by any element of S, since $1 \in MM'$, so ss' and $s + s'$ are integral over R. □

Corollary 4.8 (To Cayley-Hamilton)**.** *If M is a finitely generated R-module and I is an ideal of R such that $IM = M$ then $\exists r \in I$ such that $(1 - r)M = 0$.*

Proof. By CH, we get $p(x) \in R[x]$ with $x^n + p_1 x^{n-1} + \ldots + p_n$ with $p_j \in I^J$ such that $p(\mathrm{id})M = 0$, that is, $(1 + p_1 + \ldots + p_n)\,\mathrm{id}\, M = 0$, so set $r = -(p_1 + \ldots + p_n) \in I$. So $(1 - r)M = 0$. □

Definition 4.6 (Jacobson Radical)**.** *The Jacobson radical of R is the intersection of all maximal ideals.*

eg, $R = \mathbb{Z}$, then the Jacobson Radical is (0). If R is local, then the Jacobson Radical is the unique maximal ideal.

Corollary 4.9 (Nakayama's Lemma)**.** *Let I be an ideal contained in the Jacobson radical of R and let M be a finitely generated R-module.*

1. *If $IM = M$ then $M = 0$.*
2. *If $m_1, \ldots, m_n \in M$ have images in M/IM that generate M/IM as an R-module, then $m_1, \ldots, m_n$ generated M as an R-module.*

Proof.
1. By the corollary, $\exists r \in I$ such that $(1 - r)M = 0$, since $(1 - r)$ is not in any maximal ideal (as r is in all of them), we have $1 - r$ is a unit of R, so $M = 0$.
2. Suppose that $\bar{m}_1, \ldots, \bar{m}_n$ generate M/IM. Let $N = M/(\sum Rm_i)$. Then $N/IN = M/(IM + \sum Rm_i) = M/M = 0$, so $IN = N$, so $N = 0$.

□

Mostly, we use this in the case (R, P) is local, then M/PM is an R/P-module, and R/P is a field, so it is a vector space.

Application: If (R, P) is local, then $PM = M \Rightarrow M = 0$. ie, if $0 = M/PM$, then $M = 0$. ie, if $M/PM = R/P \otimes_R M = 0$, then $M = 0$.

Corollary 4.10. *If M and N are f.g. R-modules and $M \otimes_R N = 0$ then $\mathrm{Ann}_R M + \mathrm{Ann}_R N = R$, in particular, if R is local, then $M = 0$ or $N = 0$.*

Proof. We first prove the local case. Suppose $M \otimes_R N = 0$ but $M \neq 0$. Then Nakayama says that $M/PM \neq 0$. Now M/PM is an R/P-vector space, so there exists a surjection $M/PM \to R/P$ and thus there exists a surjection $M \to R/P$. So $0 = M \otimes_R N \to R/P \otimes_R N$ is surjective, since $\otimes$ is right exact, so $R/P \otimes_R N = 0$, so $N/PM = 0$, thus $PN = N$ so $N = 0$.

Now suppose that R is general. $M \otimes_R N = 0$ but $\operatorname{Ann}_R M + \operatorname{Ann}_R N \neq R$. Then there exists prime ideal P with $P \supseteq \operatorname{Ann}_R M + \operatorname{Ann}_R N$. Then $M_P \otimes_{R_P} N_P = 0$, so WLOG, $M_P = 0$, so $M = 0$ since $\operatorname{Ann}_R M \subseteq P$. But then $\operatorname{Ann}_R M = R$, contradiction. □

Recall that we shows that integral closure is an R-subalgebra of S. Next: Integral closure commutes with localization.

Proposition 4.11. *Let $R \subseteq S$ be rings and let U be a multiplicatively closed subset of R. If S' is the integral closure of R in S, then $S'[U^{-1}]$ is the integral closure of $R[U^{-1}]$ in $S[U^{-1}]$.*

Proof. Any element of S integral over R is integral over $R[U^{-1}]$, so S' is integral over $R[U^{-1}]$ and thus, $S'[U^{-1}]$ is integral over $R[U^{-1}]$. So we just need to show that if $s/u \in S[U^{-1}]$ is integral over $R[U^{-1}]$, then there exists $u' \in U$ with $su' \in S'$ (then $s/u = su'/uu' \in S'[U^{-1}]$).

If $(s/u)^n + r_1/u_1(s/u)^{n-1} + \ldots + r_n/u_n = 0$, multiply by $(uu_1 \ldots u_n)^n$ to get $(su_1 \ldots u_n)^n + \ldots + r_n(uu_1 \ldots u_n)^n = 0$, so $su_1 \ldots u_n$ is integral over R, and $u_1 \ldots u_n \in U$. □

Warning: If R is a Nötherian domain, then the integral closure of R in its quotient field is not necessarily Nötherian.

It is Nötherian if the integral closure is a finitely generated R-algebra ($\Rightarrow$ R-module). Also Nötherian if R is a finitely generated domain containing a field or the integers (Nöther)

eg, $R = k[x_1, \ldots, x_n]/I$, the normalization is of the form $k[y_1, \ldots, y_m]/J$.

Next: relationship between the primes in the integral closure of R and the primes in R.

Proposition 4.12 (Lying Over and Going Up)**.** *Suppose $R \subseteq S$ is an integral extension of rings, given a prime $P \subseteq R$¡ then there exists $Q \subseteq S$ prime with $Q \cap R = P$. (Lying Over)*

Also, Q may be chosen to contain any ideal $Q_1 \subseteq S$ with $Q_1 \cap R \subseteq P$. (Going Up)

eg, $R = \mathbb{Z}$, $S = \mathbb{Z}[\sqrt{2}]$ and $P = (7)$.

Proof. Factor out Q_1 and $R \cap Q_1$, to see that we just need to find a prime Q in S with $R \cap Q = P$. Let $U = R \setminus P$, so $R[U^{-1}] = R_P$. If we show $\exists Q' \in S[U^{-1}]$ with $Q' \cap R_P = P_p$, then since $Q' = Q[U^{-1}]$ for some prime Q of S, we would have $Q \cap R = P$, so we can assume that R is local with maximal ideal P.

Then, if $PS \neq S$, any maximal ideal Q of S containing PS will have $P \subseteq Q \cap R$, so $P = Q \cap R$. So we just need $PS \neq S$.

If $PS = S$, then $1 = \sum_{i=1}^{\ell} s_i p_i$, and let S' be the R-algebra generated by $\{s_1, \ldots, s_\ell\}$, then $1 \in PS'$ so $PS' = S'$ and S' is a f.g. R-module, since it is a finitely generated R-algebra over R, so by Nakayama, $S' = 0$, which is a contradiction, so $PS \neq S$. $\square$

Proposition 4.13. *Let $R \subseteq S$ be domains, if $K(S)$ is algebraic over $K(R)$, then every nonzero or S intersects R nontrivially.*

If $R \subseteq S$ is an integral extension of domains, then S is a field iff R is a field. Equivalently, if S is an integral R-algebra, P a prime of S, then P is a maximal ideal of S iff $P \cap R$ is a maximal ideal of R.

Proof. For the first statement, if sufficies to show it for a principal ideal bS of S. If $b \in S$, then there exist $a_i \in K(R)$ with $\sum_{i=0}^{n} a_i b^i = 0$. Clearing denominators and dividing by a power of b if necessary, we get $\sum_{i=0}^{m} a_i' b^i = 0$ with $a_0' \neq 0$, $a_i' \in R$. Then $a_0' \in bS \cap R$, $a_0' \neq 0$, so the ideal generated by b intersects R nontrivially.

If $R \subseteq S$ is an integral extension of domains, then $K(S)$ is alg over $K(R)$, if $s/u \in K(S)$, then $\exists a_i \in R$ with $\sum a_i s^i = 0$, so is alg over R (IOU) and $\sum b_j u^j = 0 \Rightarrow \sum_{i=1}^{m} b_j u^{j-m}$

Suppose R is a field. Let P be a maximal ideal in S. Then $P \cap R \neq \{0\}$, so $P \cap R = R$, this contains 1, so $P = S$.

Suppose instead that S is a field. Let P be a prime of R. Then by Lying Over, there is a prime Q of S with $Q \cap R = P$. But Q must equal (0), so $P = (0) \cap R = (0)$. So the only prime in R is (0), and R is a field.

Finally, take S/P and $R/(P \cap R)$. The statement follows from the field statement once we check that S/P is integral over $R/(P \cap R)$. This is because "integral dependence persists mod P", ie, if $x^n + \sum a_i x^i = 0$, then $\bar{x}^n + \sum_{i=0}^{n-1} \bar{a}_i \bar{x}^i = 0$ in S/P, and $\bar{a}_i = a_i \in R/(P \cap R)$. $\square$

Corollary 4.14 (Incompatibility)**.** *Suppose $R \subseteq S$ is an integral extension of rings. Two distinct primes of S having the same intersection with R are incomparable, ie, neither is contained in the other.*

Without integrality, we have, for example, $k \subseteq k[x, y]$, $(0) = k \cap (x) = k \cap (x, y)$, but $(x) \subseteq (x, y)$.

Proof. If $Q \subseteq Q_1 \subseteq S$ with $Q \cap R = Q_1 \cap R = P \subseteq R$, factor out $P \subseteq R$, and $Q \subseteq S$. Then we get 0 in R/P equals $0 \subset Q_1/Q \subset S/Q$. So we are in the case where R' and S' are domains. S' is still integral over R', so $K(S')$ is alg over $K(R')$, so if $Q_1 \neq Q = 0$, $Q_1 \cap R \neq (0)$, contradiction. So $Q_1 = Q = 0$ in S. $\square$

5 Blowup Algebra

<u>Geometric Motivation</u>

$\mathrm{Bl}_0 \mathbb{C}^2$ "the blowup of $\mathbb{C}^2$ at 0". We want to be able to take a curve and separate out the strands going through the origin, we'll cut out the origin and

glue in a $\mathbb{P}^1$. Algebraically, we replace $\mathbb{C}[x,y]$ by $\mathbb{C}[x,y,u,v]/(xv-yu)$, so we replace $\mathbb{C}^2$ by $V(xv-yu) \subseteq \mathbb{C}^2 \times \mathbb{P}^2$.

If $(x,y) \neq (0,0)$, then WLOG, $x \neq 0$, so if $xv - yu = 0$, then $v = y/xu$. So if $y \neq 0$, $(u:v) = (1:x/y) = (x:y)$. If $y = 0$, then $(u:v) = (1:0) = (x:y)$. So if $(x,y) \neq (0,0)$, there is a unique $(u:v)$ with $(x,y) \times (u:v) \in V(xv-yu)$. If $(x,y) = (0,0)$, then there are no conditions, so any $(0,0) \times (u:v) \in V(xv-yu)$.

Ie, consider the map $\pi : \mathrm{Bl}_0 \mathbb{C}^2 \to \mathbb{C}^2$ by $(x,y) \times (u:v) \to (x,y)$, this map is 1-1 away from the origin, and $\pi^{-1}(0,0) = \mathbb{P}^1$, the "exceptional divisor".

Now $\mathbb{C}[x,y,u,v]/(xv-yu) \simeq \mathbb{C}[x,y,xt,yt] \subseteq \mathbb{C}[x,y,t]$, $\deg t = 1, \deg x = \deg y = 0$.

Definition 5.1 (Blow-Up Algebras)**.** *If R is a ring and I is an ideal, then the blow-up algebra of I in R is the R-algebra $B_I(R) = R \oplus I \oplus I^2 \oplus \ldots \simeq R[It] \subseteq R[t]$.*

eg, $B_{(x,y)}\mathbb{C}[x,y]$ is the coordinate ring of $\mathrm{Bl}_0 \mathbb{C}^2$.

Set $\deg(r) = 0$ for $r \in R$ and $\deg(t) = 1$. Then $B_I R$ is a $\mathbb{Z}$-graded ring.

The ideal $I \subseteq B_I(R)$ is homogeneous, thus the quotient $B_I(R)/I$ is graded.

Definition 5.2 (Associated Graded Ring)**.** $\mathrm{gr}_I R = R[It]/IR[It]$ *is the asscia-ated graded ring of R.*

[Can also do for any diltration $R \supsetneq I_1 \supsetneq I_2 \supsetneq \ldots$ with $I_j I_k \subseteq I_{j+k}$.]

For $\mathbb{C}[x,y,tx,ty]/(x,y) \simeq \mathbb{C}[x,y,u,v]/(xv-yu,x,y) \simeq \mathbb{C}[u,v] = \mathrm{gr}_{(x,y)} \mathbb{C}[x,y]$, the coordinate ring of $\mathbb{P}^1$. We can also do this for modules:

Definition 5.3. *Let R be a ring, M an R-module, and I an ideal of R, then $\mathscr{I} : M = M_0 \supset M_1 \supset M_2 \supset \ldots$ is a filtration of R-modules. It is an I-filtration if $IM_i \subseteq M_{i+1}$ for all $i > 0$ and it is I-stable if $\exists n > 0$ such that $\forall i \geq 0$, $IM_{n+i} = M_{n+i+1} = I^{i+1} M_n$.*

OWED RESULT: If $R \subset S$ is an integral extension of domains, then $K(S)$ is algebraic over $K(R)$. Suppose $s_1/s_2 \in K(S)$. Then there exist a_i, b_j with $\sum_{i=0}^m a_i s_i^i = 0$, $a_m = 1$ and $\sum_{j=0}^n b_j s_2^j = 0$ with $b_n = 1$ and $b_0 \neq 0$. Then $\sum_{j=0}^n b_j/b_0 s_2^{j-n} = 0 = \sum_{j=0}^n b_j/b_0 (1/s_2)^{n-j}$, this shows that $1/s_2$ is integral over $K(R)$, so $s_1/s_2 = s_1 * 1/s_2$ is integral over $K(R)$.

Definition 5.4. *If $\mathscr{I}$ is an I-filtration, then $\mathrm{gr}_I M = M/M_1 \oplus M_1/M_2 \oplus \ldots$ and $\mathrm{Bl}_{\mathscr{I}} M = M \oplus M_1 \oplus \ldots$.*

Note: $\mathrm{gr}_I R$ is an R/I-algebra. If I is finitely generated, then $\mathrm{gr}_I R$ is a finitely generated R/I-algebra. If I is a maximal ideal, then $\mathrm{gr}_I R$ is a finitely generated algebra over a field.

Also $\mathrm{gr}_{\mathscr{I}} M$ is a graded $\mathrm{gr}_I R$ module.

Proposition 5.1. *Let I be an ideal in R and let M be a finitely generated R-module. If $\mathscr{I} : M = M_0 \supset M_1 \supset \ldots$ is an I-stable filtration by finitely generated R-submodules of M, then $\mathrm{gr}_{\mathscr{I}} M$ is a finitely generated module over $\mathrm{gr}_I R$.*

Proof. Suppose $IM_1 = M_{i+1}$ for $i \geq n$. Then $(I/I^2)(M_i/M_{i+1}) = M_{i+1}/M_{i+2}$ for $i \geq n$. So the union of any set of generateors for M_i/M_{i+1} $0 \leq i \leq n$ generates $\mathrm{gr}_{\mathscr{I}} M$ as a $\mathrm{gr}_I R$-module.

Since the M_i are finitely generated R-modules, so are the M_i/M_{i+1}, so we get a finite set of generators. □

Proposition 5.2. *Let R be a ring, $I \subseteq R$ an ideal, M a finitely generated R-module with I-filtration $\mathscr{I} = M_0 \supseteq M_1 \supseteq \ldots$ by finitely generated M_i.*

Then the filtration is I-stable iff the $B_I R$-module $B_{\mathscr{I}} M$ is finitely generated.

Proof. If $B_{\mathscr{I}} M$ is finitely generated, then its genertaors appear in the first n steps for some n, so $B_{\mathscr{I}} M$ is gneerated by $M_0, \ldots, M_n$. So $M_n \oplus \ldots$ is generated, as a $B_{\mathscr{I}} R$-module, by M_n. This means that $M_{n+1} = I^i M_n$ for $i \geq 0$ so $\mathscr{I}$ is I-stable.

Conversely, if $\mathscr{I}$ is I-stable, then $\exists n$ such that $I^i M_n = M_{n+i}$ for all $i \geq 0$, so a generating set for $M_0, \ldots, M_n$ generated $B_{\mathscr{I}} M$. □

Lemma 5.3 (Artin-Rees)**.** *Let R be a Nötherian ring, $I \subseteq R$ an ideal, and let $M' \subset M$ be finitely generated R-modules. IF $M = M_0 \supset M_1 \supset \ldots$ isw an I-stable filtration, then the induced filtration $M'_0 = M' \subset M'_1 = M_1 \cap M' \supset \ldots$ is also I-stable, so $\exists n$ such that $M' \cap M_{n+i} = I^i(M' \cap M_n)$.*

Note: IF R is Nötherian, then so is $B_I R$, since I is finitely generated. So $B_I R$ is a finitely generated R-algebra, so is Nötherian.

Proof. Let $\mathscr{I}' = M' = M'_0 \supset M'_1 \supset \ldots$. $B_{\mathscr{I}'} M'$ is naturally a $B_I R$ submodule of $B_{\mathscr{I}} M$. If $\mathscr{I}$ is stable, then $B_{\mathscr{I}} M$ is a finitely generated $B_I R$-module, so all submodules are finitely generated and, in particular, $B_{\mathscr{I}'} M'$ is finitely generated, so $\mathscr{I}'$ is I-stable. □

Q: Can we have $0 \neq I^5 = I^{20}$ in a nice ring? If so, actually have $I^j = I^5$ for all $j \geq 5$. So we'd get $\cap_{j \geq 1} I^j = I^5$.

Corollary 5.4 (Krull Intersection Theorem)**.** *Let $I \subset R$ be an ideal in a Nötherian ring. If M is a finitely generated R-module, then there is an $r \in I$ such that $(1-r)(\cap_{j=1}^{\infty} I^j M) = 0$. If R is a domain or a local ring, and I is a proper ideal, then $\cap_{j=1}^{\infty} I^j = 0$.*

Proof. For any P, $\cap_{j \geq 1} I^j M = (\cap_{j \geq 1} I^j M) \cap I^{p+1} M$, now Artin-Rees applied to $\cap I^j M \subset M$ for the I-stable filtration $M_j = I^j M$ says that $\exists p$ such that $I(\cap_{j \geq 0} I^j M \cap I^p M) = (\cap_{j \geq 0} I^j M) \cap I^{p+1} M = \cap_{j \geq 0} I^j M$. ie, $\exists p$ such that $I(\cap_{j \geq 0} I^j M) = \cap_{j \geq 0} (I^j M)$. So $\exists r \in I$ such that $(1-r) \cap_{j \geq 0} I^j M = 0$. □

6 Flatness

A Flat Family: A "family" of varieties is one that varies with parameters.

Eg: $V(x^2 - a^2)$ for $a \in k$ is $\{a, -a\}$.

Eg: $V(x) \cup V(y - ax) = V(x(y - ax))$, two lines through the origin.

A way to think about $V(x^2 - a^2)$ is as a union of two lines projected down to a line.

A family, then, is a map of varieties $\pi : Y \to X$ with the fibers $\pi^{-1}(x) \subset Y$ for $x \in X$.

Corresponding map of rings $R \to S$ in the other direction. IE, $k[a] \to k[x, a]/(x^2 - a^2)$. So a family over $\mathrm{Spec}(R)$ is an R-algebra S.

Definition 6.1 (Fiber)**.** *The fiber over any prime $P \subset R$ is $K(R/P) \otimes_R S$*

eg $(a - 7) \subseteq k[a]$ has fiber $k[a]/(a - 7) \otimes_{k[a]} k[a, x]/(x^2 - a^2) \simeq k[a, x]/(x^2 - a^2, a - 7) \simeq k[x]/(x^2 - 49)$ is the ring of $\{7, -7\}$.

eg, $\mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-algebra, so $\mathrm{Spec}(\mathbb{Z}_2) \to \mathrm{Spec}(\mathbb{Z})$ is a family. The fiber over 7 is $\mathbb{Z}_7 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \simeq 0$. So the fiber over (2) is $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2$ and is trivial elsewhere.

We replace locally trivial is flat. A family is nice if it is flat, that is, S is a flat R-module.

Recall that if $0 \to A \to B \to C \to 0$ is a ses of R-mods, then $A \otimes M \to B \otimes M \to C \otimes M \to 0$ is exact for any R-module M. If $0 \to A \otimes M \to B \otimes M$ is exact, then M is called a flat R-module.

eg $R = k[x]$ and $S = k[x, y]/(x - y)$. Check: S is flat (since $S \simeq k[x] = R$ as an R-module).

Free R-modules are always flat.

eg: $S = k[x, t]/(tx - 1)$, $R = k[t]$. Then $S \simeq k[t, t^{-1}]$, and $R[U^{-1}]$ is flat for all multiplicative sets $U \subset R$.

eg: $R = k[a, b]$, $S = R[a, b, x, y]/(ax + by)$, then S is an R-module but is not flat!

Important Example: "Gröbner Degeneration". If $S = k[x_1, \ldots, x_n]$, and $I \subset S$ is an ideal. Let $w \in \mathbb{R}^n$ and consider $\leq_w$ where $x^u < x^v$ if $w \cdot u < w \cdot v$ or (other condition)

Gröbner theory studies the ideal $\in_w (I)$. So we define, given $f \in S$, $f = \sum c_u x^u$, set $\tilde{f} = f(x_i/t^{w_1}, \ldots, x_n/t^{w_n})t^b \in S[t]$ where $b = \max_{c_u \neq 0} w \cdot u$. ie, $\tilde{f} = \sum c_u x^u t^{b - w \cdot u}$.

So if $S = k[x, y]$, $w = (2, 3)$ and $f = x^2 + y^3$, then $\tilde{f} = x^3 + y^2$, if $f = x^3 + 3xy$ then $\tilde{F} = x^3 + 3xyt$.

Define $I_t \subset S[t]$ to be $I_t = \langle \tilde{f} | f \in I \rangle$, then $I_t|_{t=1} = I$ and $I_t|_{t=0} = \in_w (I)$. So $S[t]/I_t$ is a $k[t]$-module defining a family. Check that, for all $a \neq 0$, the fiber over $t = a$ is isomorphic to S/I.

Lemma 6.1. *$S[t]/I_t$ is a free, and thus flat, $k[t]$-module.*

Recall: $B = \{x^u | x^u \notin \in_w (I)\}$ is a basis for S/I as a k-vector space.

Proof. We claim that B is a $k[t]$ basis for $S[t]/I_t$. That is, $S[t]/I_t \simeq \oplus k[t]x^u$ over $x^u \in B$.

The key point is that if $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis for I, then $\{\tilde{g_1}, \ldots, \tilde{g_r}\}$ generate I_t and $\tilde{g}_i = \in_w (g_i) + t(\text{other stuff})$. Given $f \in S[t]$, dividing by $\{\tilde{g}_i\}$ gives a polynomial $\sum p_u(t)x^u$.

"linear independence" as before. If $f = \sum p_u(t)x^u = 0$ in $S[t]/I_t$, then $f = t^k(\sum p'_u(t)x^u)$ are not all divisible by G so equals $\sum q(x, t)\tilde{g}_i$. $\square$

Summary: $S[t]/I_t$ is a free and thus flat R-module, so $V(I_t) \subseteq k^n \times k$ is a flat family.

We say this gives a Gröbner Degeneration from $V(I)$ to $V(\in (I))$.

Check: $S[t]/I_t \otimes_{k[t]} k[t]/(t) \simeq S/\in_w (I)$ and $S[t]/I_t \otimes_{k[t]} k[t]/(t-a) \simeq S/I$.

eg: $I = (xy - y^2) \subset k[x,y]$, $w = (2,1)$, so $I_t = (xy - t^2y^2)$, we get the union of the x axis and a line of slope $1/t^2$, and $\in_w (I) = (xy)$.

eg: $I = (x^2 + y^2 - 4) \subseteq \mathbb{C}[x,y]$, then $I_t = (x^2 + t^2y^2 - 4t^2) \subseteq \mathbb{C}[x,y,t]$, $\in_{\leq} (T) = (x^2)$.

Let $R = k[a,b]$ and $S = k[a,b,x,y]/(ax+by)$, and S is not flat. Look at $(a,b) \otimes S \to R \otimes S$.

<u>Tor</u>

Flatness says that $0 \to A \to B \to C \to 0$ exact implies $0 \to A \otimes M \to B \otimes M \to C \otimes M \to 0$, but we get all but the first anyway.

If M is not flat, we would like to define $\mathrm{Tor}_1(M,C) \to \ker(A \otimes M \to B \otimes M)$.

'General Homological Algebra'

If F is a right exact functor from R-modules to R-modules, then given $0 \to A \to B \to C \to 0$ we get $\ldots \to L_1FB \to L_1FC \to FA \to FB \to FC \to 0$.

Definition 6.2. *Let P: $\ldots \to P_2 \to P_1 \to P_0 \to M \to 0$ be a projective resolution of an R-module M (ie P is exact with each P_i projective).*

If $R = k[x_1, \ldots, x_n]$ and $M = R/I$ ten we can construct a free resolution using Gröbner Bases by Schreyer's Algorithm.

Definition 6.3. *Given a projective resolution P, define FP to be $\ldots \to FP_2 \to FP_1 \to FP_0 \to FM \to 0$. This is still a chain complex, so we take homology, and $LF_i = \ker F\varphi_i / \operatorname{Im} F\varphi_{i+1}$.*

For us: $\mathrm{Tor}_i(M,N) = LF_i(N)$ where F is $-\otimes_R M$. So to compute $\mathrm{Tor}_i(M,N)$, we compute a projective resolution of N, tensor with M, and take the ith homology.

Basic Facts:

1. It doesn't matter what resolution we take.
2. $\mathrm{Tor}_i(M,N) = \mathrm{Tor}_i(N,M)$.
3. $\mathrm{Tor}_0(M,N) = M \otimes_R N$.
4. If M is projective, then $\mathrm{Tor}_i(M,N) = 0$ for all $i > 1$.

Examples: If $x \in R$ is a nonzero divisor then $0 \to R \xrightarrow{x} R \to R/(x) \to 0$. Claim: This is a free resolution of $R/(x)$. Thus $\mathrm{Tor}_i(R/(x),M) = R/(x) \otimes_R M = M/xM$ if $i = 0$, is $\ker(M \xrightarrow{x} M) = (0 :_m x) = \{m \in M : xm = 0\}$ if $i = 1$ and 0 else.

eg. $R = k[x,y]$ and $M = N = k[x,y]/(x,y) \simeq k$. What is $\mathrm{Tor}_i^R(k,k)$. Then $0 \leftarrow M \leftarrow R \overset{(x,y)}{\leftarrow} R^2 \overset{(y,-x)^t}{\leftarrow} R \leftarrow 0$ is a free resolution.

So then $\mathrm{Tor}_i(k,k) = k$ if $i = 0$, k^2 is $i = 1$ and k if $i = 2$, 0 else. In general, if $R = k[x_1, \ldots, x_n]$ and $M = R/(x_1, \ldots, x_n)$, then $\mathrm{Tor}_i(M, N) = k^{\beta_i}$ for some β_i, and we call the β_i the Betti numbers.

A long exact sequence: If $0 \to A \to B \to C \to 0$ then we get $\mathrm{Tor}_i(A, M) \to \mathrm{Tor}_i(B, M) \to \mathrm{Tor}_i(C, M) \to \mathrm{Tor}_{i-1}(A, M) \to \ldots \to \mathrm{Tor}_1(C, M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$.

More facts about Tor: If S is a flat R-algebra, then $S \otimes_R \mathrm{Tor}_i^R(M, N) = \mathrm{Tor}_i^S(S \otimes_R M, S \otimes_R N)$.

If we have a short exact sequence $0 \to A \to B \to C \to 0$ we get a long exact sequence $\to \mathrm{Tor}_i^R(A, M) \to \mathrm{Tor}_i^R(B, M) \to \mathrm{Tor}_i^R(C, M) \to \mathrm{Tor}_{i-1}^R(A, M) \to \ldots \to \mathrm{Tor}_1(B, M) \to \mathrm{Tor}_1(C, M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$.

Proposition 6.2. *Let R be a ring and M an R-module. If I is an ideal of R then the multiplicative map $I \otimes_R M \to M$ is an injection iff $\mathrm{Tor}_i^R(R/I, M) \to 0$.*

The module M is flat iff this condition is satisfied for all finitely generated I.

Proof. Consider the ses $0 \to I \to R \to R/I \to 0$. From this we get a long exact sequence $\mathrm{Tor}_1(R, M) \to \mathrm{Tor}(R/I, M) \to I \otimes M \to R \otimes M = M$.

As $\mathrm{Tor}_1(R, M) = 0$, $I \otimes M \to M$ is injective iff $\mathrm{Tor}_1(R/I, M) = \ker(I \otimes M \to M)$ is zero.

Recall that M is flat iff $M \otimes N' \to M \otimes N$ is an inclusion for all inclusions $N' \subseteq N$.

First we assume this for all N' finitely generated I and $N = R$. We must show that this implies the general condition for $N' \subseteq N$. First, let I be a general ideal of R and $x \in I \otimes M$. Then $x = \sum_{i=1}^s r_i \otimes m_i$. Let I' be the ideal generated by $< r_1, \ldots, r_s >$. Then $x \in I' \otimes M \to M$ is an inclusion, so $x \neq 0$ in M.

Now consider $N' \subseteq N$. BY the same argument we may assume that N is finitely generated. ie, $x \in N' \otimes M$, then $x = \sum n_i \otimes m_i$, let $\tilde{N}$ be the submodule generated by the n_i and any necessary relations. We can thus assume that N is finitely generated. So we can find a filtration $N' = N_0 \subset N_1 \subset \ldots \subset N_r = N$ with each N_i/N_{i-1} cyclic.

It suffices to show that $N_i \otimes M \to N_{i+1} \otimes M$ is an inclusion, so we may assume that $N/N' \simeq Rx \simeq R/I$. Now from $0 \to N' \to N \to N/N' \to 0$ we get $\mathrm{Tor}_1(N/N', M) \to N' \otimes M \to N \otimes M$. $\mathrm{Tor}_1(N/N', M) = \mathrm{Tor}_1(R/I, M) = 0$ by hypothesis. So $N' \otimes M \to N \otimes M$ is an inclusion for arbitrary $N' \subseteq N$, so M is flat. $\square$

The point was that $I \otimes M \to M$ being an inclusion for all finitely generated I implies that $N' \otimes M \to N \otimes M$ is an inclusion for all $N' \subseteq N$.

So to check flatness, it is enough to check finitely generated ideals.

Corollary 6.3. *Let k be a field and $R = k[t]/t^2$, and M an R-module. Then M is flat iff multiplication by t from M to tM induces an isomorphism $M/tM \to tM$.*

Proof. The only nonzero ideal in R is (t). So M is flat iff $(t) \otimes M \to M$ is an injection. As $(t) \simeq R/(t)$ as an R-module by $t \leftrightarrow 1$, we have $(t) \otimes M \simeq$

$R/(t) \otimes M \simeq M/tM$, so the map $M/tM \to tM$ by $m \mapsto tm$ is the composition $R/t \otimes M \to t \otimes M \to M$. So it is injective. $\square$

Corollary 6.4. *If $a \in R$ is a nzd in R and M is a flat R-module, then a is a nzd on M.*

If R is a PID, then the converse is true: M is flat iff M is torsion free.

Proof. Let $a \in R$ be a nzd and M flat. $I = Ra \simeq R$ by $1 \mapsto a$. So we have $R \otimes M \to I \otimes M \to R \otimes M$ by $1 \otimes m \to a \otimes m \to a \otimes m$, so $m \mapsto am$. Simce the map $m \mapsto am$ is injective, a is a nzd on M.

Suppose that R is a PID and M is torsion free, so no element of R annihilates an element of M. Then for any $a \neq 0$ in R, $Ra \otimes M \to M$ is an injection, since $0 \otimes M \to M$ is an injection as well, this means that $I \otimes M \to M$ is an inclusion for all finitely generated I, thus M is flat. $\square$

Definition 6.4 (Rees Algebra)**.** *The Rees Algebra of R with respect to I, $\mathscr{R}[R, I] = R[t, t^{-1}I] \subseteq R[t, t^{-1}]$. It is $\sum_{n=-\infty}^{\infty} I^n t^{-n}$ with $I^n = R$ for $n \leq 0$.*

If R is a k-algebra (k a field) we'll see that $\mathscr{R}[R, I]$ is a flat $k[t]$-algebra.

Facts: $\mathscr{R}[R, I]/i\mathscr{R}[R, I] = \mathrm{gr}_I R = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \ldots$.

If $a \neq 0$ in R, then $\mathscr{R}[R, I]/(t - a)\mathscr{R}[R, I] \simeq R$.

So $\mathscr{R}[R, I]$ is a family over $[t]$ with fiber over $t = 0$ $\mathrm{gr}_I R$ and fiber over everything else R.

Lemma 6.5. *If R is a k-algebra, then $S = \mathscr{R}[R, I]$ is flat over $k[t]$.*

If $\cap_{d=1}^{\infty} I^d = 0$ then every element of the form $1 - ts$ with $s \in S$ is a nzd on $\mathscr{R}[R, I]$.

Proof. Since $k[t]$ is a PID, it suffices to observe that S is torsion free as $k[t]$-module. This is immediate from the fact that $S = R[t, It^{-1}] \subseteq R[t, t^{-1}]$.

For the second statement, suppose first that $p(1 - ts) = 0 \in S$. This means that $p \in (t)$, $p = qt$. t is a nzd on S, so $q(1 - ts) = 0$ in S, so $q \in t$, so $p \in t^2$. Continue to get that $p \in t^n S$ for all n.

Now $p = \sum_{i=-j}^{j} p_i t^j$. Since $p \in t^n S$ for all n, we must have $p_i \in I^m$ for all m. $\square$

What to take away: Flatness is a niceness property, and flat families preserve a lot of properties (ie, dimension)

7 Completions

The basic idea is that the open sets in the Zariski topology are too big, so we look for smaller neighborhoods.

eq if $R = k[x_1, \ldots, x_n]$ and $\mathfrak{m} = (x_1, \ldots, x_n)$, then $R_{\mathfrak{m}} = \{f/g : g(0) \neq 0\}$. We replace this by $\hat{R} = k[[x_1, \ldots, x_n]]$ formal power series, and we get a natural map $R_{\mathfrak{m}} \to \hat{R}$.

One advantage is that we get a version of the inverse function theorem.

Definition 7.1 (Inverse Limit)**.** *If $\{G_i | i \in \mathbb{N}\}$ is a sequence of abelian groups with homomorphisms $\varphi_i : G_i \to G_{i-1}$. Then $\varprojlim G_i = \{g \in \prod_{i=1}^{\infty} G_i | \varphi_i(g_i) = g_{i-1}\}$ is the inverse limit, which is an abelian group under coordinatewise addition.*

We will be interested in the case where we start with a ring R and a filtration $\mathfrak{m}_1 \supset \ldots \mathfrak{m}_n \subset \ldots$ of ideals and set $G_i = R/\mathfrak{m}_i$. Write $\hat{R} = \varprojlim R/\mathfrak{m}_i$.

$\hat{R}$ is a ring by coordinate multiplication. Most important case is $\mathfrak{m}_i = \mathfrak{m}^i$ for some ideal $\mathfrak{m} \subset R$. Notation is $\hat{R}_{\mathfrak{m}}$. eg $R = k[x]$, $\mathfrak{m} = (x)$, then $\hat{R}_{\mathfrak{m}} = \varprojlim k[x]/x^i$.

Claim: $\hat{R}_{\mathfrak{m}} = k[[x]]$.

Proof. $\varphi : k[[x]] \to \hat{R}_{\mathfrak{m}}$, $a \to (b_1, b_2, \ldots)$ by $\sum a_i x^i \mapsto b_i = \sum_{n=0}^{i-1} a_n x^n$.

This is a well-defined homomorphism, so we just need to check that it is iso. For the inverse map, given $b = (b_1, \ldots) \in \hat{R}_{\mathfrak{m}}$, each b_i has a representation of the form $\sum_{j=0}^{i-1} a_{ij} x^j$ and if $k < \ell$ then $a_{kj} = a_{\ell j}$ for $j < k$. Define $\psi : \hat{R}_{\mathfrak{m}} \to k[[x]]$ by $b \mapsto \sum_{j=0}^{\infty} a_{ij} x^j$. $\square$

Definition 7.2 (Complete with respect to $\mathfrak{m}$)**.** *There is a natural map, $R \to \hat{R}_{\mathfrak{m}}$ by $r \mapsto (r, r, r, \ldots)$, if this is an isomrophism, then R is complete.*

Theorem 7.1 (Cohen Structure Theorem)**.** *If R is a complete local ring containing a field, then $R = k[[x_1, \ldots, x_n]]/I$ for some I.*

eg, the p-adics, $p \in \mathbb{Z}$, then $\hat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^n$, with $\varphi : \mathbb{Z}/p^n \to \mathbb{Z}/p^{n-1}$ by $a \mapsto a$.

Then we can write elements of $\hat{\mathbb{Z}}_p$ as $\sum_{i=0}^{\infty} a_i p^i$ for $0 \leq a_i < p$ with addition is "add with carrying"

In $\hat{\mathbb{Z}}_2$, $1 + 2 + 4 + 8 + 16 + \ldots$ is $b = (1, 3, 7, \ldots) = (-1, -1, -1, \ldots)$, and $1 = (1, 1, 1, \ldots)$.

If we have $\mathfrak{m}_1 \supset \mathfrak{m}_2 \supset \ldots$ we get an ideal $\hat{\mathfrak{m}}_1 = \{g = (g_1, \ldots) | g_j = 0 \forall j \leq i\} \subseteq \hat{R}$. When $\mathfrak{m}_i = \mathfrak{m}^i$, then $\hat{\mathfrak{m}}_1 = \hat{\mathfrak{m}}$.

Lemma 7.2. *When $\mathfrak{m}$ is a maximal ideal in R, then $\hat{R}_{\mathfrak{m}}$ is a local ring. For any filtration, we have $\hat{R}/\hat{\mathfrak{m}}_i = R/\mathfrak{m}_i$.*

Proof. If $g \in \hat{R}/\hat{\mathfrak{m}}_i$, then map $g + \hat{\mathfrak{m}}_i \mapsto g_i + \mathfrak{m}_i$ is the "projection homomorphism"

If $\varphi(g + \hat{\mathfrak{m}}_i) = 0$ then $g_i \in \mathfrak{m}_i$, so $g_j \in \mathfrak{m}_j$ for $j < i$. So $g = (0, 0, 0, \ldots, 0, -, \ldots) + \hat{\mathfrak{m}}_i$, so $g \in \hat{\mathfrak{m}}_i$, so $g = 0$.

It is surjective, since $R \to \hat{R} \to R/\mathfrak{m}_i$ by $r \mapsto (r, r, r, r, \ldots) \to r + \mathfrak{m}_i$.

Thus $\hat{R}/\hat{\mathfrak{m}}_i \simeq R/\mathfrak{m}_i$. If $\mathfrak{m}$ is a maximal ideal in R, then $R/\mathfrak{m}$ is maximal. Thus, $\hat{R}/\hat{\mathfrak{m}}$ is a field, and so $\hat{\mathfrak{m}}$ is a maximal ideal of $\hat{R}$. We now show that if $g \in \hat{R} \setminus \hat{\mathfrak{m}}$, then g is a unit.

Note that each $R/\mathfrak{m}^i$ is a local ring with maximal ideal $\mathfrak{m}$. So if $g_i \in R/\mathfrak{m}^i \setminus \mathfrak{m}$, then g_i is a unit in $R/\mathfrak{m}^i$. If $g = (g_1, g_2, \ldots) \in \hat{R}_{\mathfrak{m}} \setminus \hat{\mathfrak{m}}$, then $g_1 \neq 0$, so each $g_i \notin \mathfrak{m}R/\mathfrak{m}^i$.

Since $g_i = g_j \bmod \mathfrak{m}$, then $g_i^{-1} = g_j^{-1} \bmod \mathfrak{m}$, so set $g^{-1} = (g_1^{-1}, \ldots)$, and note that $gg^{-1} = (1, 1, 1, \ldots)$. $\square$

eg $k[[x]]$ is local with maximal ideal (x). $\hat{\mathbb{Z}}_p$ is local with maximal ideal (p).
Note: If $\mathfrak{m}$ is a maximal ideal, $R/\mathfrak{m}^i \simeq (R/\mathfrak{m}^i)_\mathfrak{m} = R_\mathfrak{m}/\mathfrak{m}\mathfrak{m}^i$.
So we get the same $\hat{R}_\mathfrak{m}$ if we localize at $\mathfrak{m}$ first.
So if $\mathfrak{m}$ is maximal, we say that $\hat{R}_\mathfrak{m}$ is a complete local ring.
Note: If R is complete with respect to $\mathfrak{m}$, then $\cap_{j=0}^{\infty} \mathfrak{m}^j = 0$.

Definition 7.3 (Convergence)**.** *A sequence $a_1, a_2, \ldots \in \hat{R}$ converges to an element $a \in \hat{R}$ if $\forall n \exists i_n$ such that $a - a_j \in \hat{\mathfrak{m}}_n$ for $j \geq i_n$, ie $a_{i_n} = (a_1, a_2, \ldots, a_n, other)$.*
A sequence is Cauchy if $\forall n \exists i_n$ such that $a_i - a_j \in \hat{\mathfrak{m}}_n$ for $i, j \geq i_n$.
A sequence converges iff it is Cauchy.

This is the usual notion of convergence in the $\mathfrak{m}$-adic topology which has a base of open sets $\{a + \hat{\mathfrak{m}}_i | a \in \hat{R}, i \geq 1\}$.

Cauchy implies Convergence: we set $a = \lim a_i$, ie, if $\{a_i\}$ is Cauchy, $a_i = (a_{i_1}, a_{i_2}, \ldots)$, set $a = (b_1, b_2, \ldots)$ with $b_n = a_{jn}$ for any $j > i_n$.

This is well defined, since if $j, k \geq i_n$, $a_j - a_k \in \hat{\mathfrak{m}}_n$ so $a_{jn} = a_{kn}$. Check $a \in \hat{R}$: If $j > i_n$, then $b_n = a_{jn}$ and $b_{n-1} = a_{jn-1}$ so $b_n = b_{n-1} \bmod \mathfrak{m}_{n-1}$.

Check: $\{a_i\}$ converges to a. Given n, $\exists i_n$ such that $\forall i, j \geq i_n$, $a_i - a_j \in \hat{\mathfrak{m}}_n$. By construction, for such an i, $a_i - a \in \hat{\mathfrak{m}}_n$, so $\forall i \geq i_n$, $a_i - a \in \hat{\mathfrak{m}}_n$, so $\{a_i\} \to a$.

From analysis: we know that if $a_i \to a$ and $b_i \to b$, then $a_i + b_i \to a + b$ and $a_i b_i \to ab$.

Application:

Proposition 7.3. *If R is complete with respect to $\mathfrak{m}$, then $U = \{1 - a | a \in \mathfrak{m}\}$ are units in R.*

Proof. If $a \in \mathfrak{m}$, set $a_i = \sum_{j=0}^{i} a^j = 1 + a + a^2 + \ldots$. Then the sequence $\{a_i\}$ is Cauchy. If $i, j > n - 1$, then $a_i - a_j \in \mathfrak{m}^n$. So it converges to some $b \in R$. And $(1 - a)a_i$ converges to $(1 - a)b$.

But $(1 - a)a_i = 1 - a^{i+1}$, so it converges to 1. $\square$

We saw this with $a = 2$ in $\hat{\mathbb{Z}}_2$, there $1 + 2 + 4 + 8 + \ldots$, so the limit of the Cauchy sequence $\sum_{j=0}^{i} 2^i$ is -1.

Corollary 7.4. *R is a local ring with maximal ideal P, then $R[[x_1, \ldots, x_n]]$ is local with maximal ideal $P + (x_1, \ldots, x_n)$.*

Proof. $R[[x_1, \ldots, x_n]] = R[\widehat{x_1, \ldots, x_n}]_{(x_1, \ldots, x_n)}$. If $f \in P + (x_1, \ldots, x_n)$, then f has constant term $f_0 \notin P$, so f_0 is a unit in R. So $f_0^{-1} f = 1 + g$ for $g \in (x_1, \ldots, x_n)$.

So $1 + g$ is a unit, thus f is a unit as well. $\square$

Definition 7.4. *Let $R = m_0 \supset m_1 \supset \ldots$ be a filtration of ideals, and let $\operatorname{gr} R$ be the associated graded ring.*

Given $f \in R$ let $m = \max\{j | f \in m_j\}$. Define $in(f) = f + m_{m+1} \in \mathfrak{m}_j/\mathfrak{m}_{j+1} \in \operatorname{gr} R$.

Proposition 7.5. *Suppose that R is a ring complete with respect to $m_1 \supset m_2 \supset \ldots$. Suppose $I \subset R$ is an ideal, $a_1, \ldots, a_s \in I$. If $in(a_1), \ldots, in(a_s)$ generate $in(I) = (in(f) | f \in I) \subset \operatorname{gr} R$. Then $\{a_1, \ldots, a_s\}$ generate I.*

Proof. Let $I' = (a_1, \ldots, a_s)$. We may assume that none of the a_i are 0. Choose $d >> 0$ so that $a_i \notin m_d$ for all i.

Given $f \in I$ with $in(f)$ of degree e, we can write $in(f) = \sum_{j=1}^{s} G_j in(a_j)$ with $G_j \in gr_m R$ homogeneous of degree $\deg(in(f)) - \deg(in(a_j))$. Take $g_1, \ldots, g_s$ with $in(g_j) = G_j$. Then $f - \sum_{j=1}^{s} g_j a_j \in m_{e+1}$.

Repeat: we can get $f' \in I'$ with $f - f' \in m_{d+1}$. Now keep repeating, noting that now $\deg(G_j) \geq e - d > 0$.

$g_j \in m_{e-d}$, so get $f - \sum_j g_j^{(0)} a_j - \sum_j g_j^{(1)} a_j - \ldots - \sum_j g_j^{(n)} a_j$ with $g_j^{(i)} \in m_{e-d+i}$.

$f^n \in m_{e+n+1}$, so the series $\sum_{i=0}^{\infty} g_j^{(i)}$ converges, and we will call the limit h_j. Now look at $f - \sum h_j a_j$. This is 0, since $\cap m_i = 0$, and so $f \in I'$, thus the a_i generate I. □

Theorem 7.6. *Let R be a Nötherian ring and let m be an ideal of R.*

1. *$\hat{R}_m$ is Nötherian.*
2. *$\hat{m}_n = m^n \hat{R}_m$, so $\operatorname{gr}_{\hat{m}} \hat{R} = \operatorname{gr}_m R$.*

Proof. Write $\operatorname{gr} \hat{R}$ for the associated graded ring of R with respect to $\hat{m}_i$. Then since $\hat{R}/\hat{m}_i \simeq R/m^i$, we have $\operatorname{gr} \hat{R} = \operatorname{gr}_m R$. Since R is Nötherian, so is R/m.

The ring $\operatorname{gr}_m R$ is finitely generated as an R/m algebra (since m is a finitely generated ideal). So $\operatorname{gr}_m R \simeq R/m[x_1, \ldots, x_\ell]/J$ for some ideal ℓ, J, thus $\operatorname{gr}_m R$ is Nötherian by the Hilbert Basis Theorem.

So $\operatorname{gr} \hat{R}$ is Nötherian. So for any ideal $I \subseteq \hat{R}$, the ideal $in(I) \subseteq \operatorname{gr} \hat{R}$ is finitely generated by the initial forms of $a_1, \ldots, a_s$, so $a_1, \ldots, a_s$ generate I, and so $\hat{R}$ is Nötherian.

To show that $\hat{m}_n = m^n \hat{R}_m$ it suffices to show that both have the same initial ideals in $\operatorname{gr} \hat{R}$. (This uses Nötherian, as we need ideals in $\operatorname{gr} \hat{R}$ to be finitely generated to apply the prop). But both initial ideals consist of all terms of degree $\geq n$. □

Theorem 7.7. *Let R be a Nötherian ring. Let I is an ideal of R.*

1. *If M is a finitely generate R-module, then the natural map $\hat{R} \otimes_R M \to \varprojlim M/I^j M = \hat{M}$ is an isomorphism.*
2. *$\hat{R}$ is a flat R-module.*

Lemma 7.8 (Hensel's Lemma)**.** *Let R be a ring that is complete with respect to an ideal m. Let $f(x) \in R[x]$. If a is an approximate root of f in the sense that $f(a) \equiv 0$ mod $f'(a)^2 m$ then there is a root b of f near a in the sense that $f(b) = 0$ and $b \equiv a$ mod $f'(a)m$.*

If $f'(a)$ is a nzd on R, then b is unique.

Most often used when $f'(a)$ is a unit.

Application

Is 8 a square in $\hat{\mathbb{Z}}_7$?

Take $c \in \hat{\mathbb{Z}}_p$. Write $c = p^n b$ where $p \not| b$. (ie $b = \sum_{i=0}^{\infty} b_i p^i$, $b_0 \neq 0$). Then c is a square iff n is even and b is a square. So we'll assume $c = \sum_{i=0}^{\infty} c_i p^i$ has $c_0 \neq 0$.

If $c = d^2$, $d = \sum_{i=0}^{\infty} d_i p^i$, then $c_0 = d_0^2 \bmod p$.

Consider $f(x) = x^2 - c$. (assume $p > 2$). Then $f(d_0) = d_0^2 - c \in (p)$. $f'(x) = 2x$, so $f'(d_0) = 2d_0 \neq 0$, so is a unit in $\hat{\mathbb{Z}}_p$. So Hensel's lemma says that there is a root of f, so c is a square.

So as $8 = 1 + 7$, and 1 is a square mod 7, 8 must be square.

Idea: use Newton's method to construct $a_1, a_2, a_3, \ldots$ by $a_{i+1} = a_i - f(a_i)/f'(a_i)$. Claim: This is a convergent sequence with limit b and $f(b) = 0$. Recall Taylor's Theorem that $f(x + y) = f(x) + f'(x)y + h(y)y^2$ for some polynomial $h(y) \in R[x][y]$.

Fact 1: If $f'(a_1)$ is a unit, so is $f'(a_i)$ for all i (assume that $f(a_i) \in m$).

$b_i = f'(a_{i+1}) - a_i = -f(a_i)/f'(a_i) = f'(a_i) + f''(a_i)b_i + h_{ai}(b_i)b_i^2$ is a unit plus something in m. As such, $f(a_i + 1)$ is a unit.

Fact 2: If $f(a_1) \in m^i$, $f(a_{i+1}) \in m^{2i}$. $f(a_{i+1}) = f(a_i + b_i) = f(a_i) + f'(a_i)b_i + h_{ai}(b_1)b_i^2 = h_a(b_1)b_i^2 \in m^{2i}$.

$f(a_{i+1}) \in m^{2i}$ implies that $b_{i+1} \in m^{2i}$, so $a_{i+1} - a_i \in m^{2i}$, so $\{a_i\}$ is Cauchy. Let b be the limit. Argue that $f(b) = 0$.

Question: What about better approximation? ie, can we replace $\mathfrak{m}$ by $\mathfrak{m}^2, \ldots, \mathfrak{m}^n$?

Yes, and the same proof/statement works, because if R is complete wrt $\mathfrak{m}$, it is complete wrt $\mathfrak{m}^n$.

Proposition 7.9 (Universal Property of Inverse Limit)**.** *If $\{G_i\}$ is a set of abelian groups with $\varphi_i : G_i \to G_{i-1}$ and H is an abelian group with $\psi_i : H \to G_i$ such that $\varphi_i \psi_i = \psi_{i-1}$, then there exists a unique map $\psi : H \to \varprojlim G_i$ such that everything commutes.*

Note: If R is a ring and S is and R-algebra that is complete with respect to $\mathfrak{n}$ and $f_1, \ldots, f_n \in \mathfrak{n}$, then $\exists!$ R-algebra homomorphism $\varphi : R[[x_1, \ldots, x_n]] \to S$ sending x_i to f_i for each i. Theorem 7.16.

8 Dimension

Definition 8.1 (Krull Dimension)**.** *The Krull dimension is the supremum of the lengths of ascending chains of distinct prime ideals.*

The motivation is: The dimension of a vector space is the length of the longest (or any maximal) chain of subspaces.

eg. Let k be a field. Then $\dim k = 0$.

$\dim k[x] = 1$, as $0 \subseteq (x)$ and if $0 \subseteq (p) \subseteq (q)$ then $(q) = (p)$.

This actually proves the following:

Lemma 8.1. *If R is a PID, then* $\dim R = 1$.

In affine algebraic geometry, the dimension of a variety $V(I) \subseteq \mathbb{A}^n$ is the length of the longest chain of subvarieties $V(I) = V_r \supset V_{r-1} \supseteq \ldots \supseteq V_0$, which is $\dim k[x_1, \ldots, x_n]/I$.

For rings of the form $R = k[x_1, \ldots, x_n]/I$ every maximal chain of primes has the same length (a ring with this property is called Catenary)

<u>Properties of Dimension</u>

1. $\dim R = \sup_P \dim R_P$ over all P prime in R.
2. Nilpotents don't affect dimension. ie, if I is a nilpotent ideal of R (so $I^k = 0$ for some k), then $\dim R = \dim R/I$.
3. Dimension is preserved by maps with finite fibers. If $R \subseteq S$ are rings such that S if a finitely generated R-module, then $\dim R = \dim S$.
4. Calibration: if k is a field, then $\dim k[x_1, \ldots, x_n] = n$.
5. If R is an affine domain over a field $R \simeq k[x_1, \ldots, x_n]/I$ for I prime, then $\dim R = \operatorname{tr\,deg}_k R$.
6. If R is Nötherian local with maximal ideal $\mathfrak{m}$, then $\dim R$ is the minimum n such that $\exists n$ elements $f_1, \ldots, f_n \in \mathfrak{m}$ not in any prime other than $\mathfrak{m}$.
7. If R is an $\mathbb{N}$-graded ring $R_0 = k$ generated in degree 1, then there exists a polynomial P such that $P(n) = \dim_k R_n$ for $n >> 0$. Then $\dim R = 1 + \deg P$. This polynomial is called the Hilbert Polynomial.

   eg, $R = k[x]$, $\deg(x) = 1$, then $P(n) = 1$ for all n, so $\dim R = 1$. This gives an algorithm to compute dimension for $R = k[x_1, \ldots, x_n]/I$.

Fact: Flat implies that the fibers have the same hilbert polynomial

By convension: if $I \subseteq R$ is an ideal, the dimension of I is the dimension of the ring R/I.

If M is an R-module, then the dimension of M is the dimension of $\operatorname{Ann} M$ (which is $\dim R/\operatorname{Ann} M$). Think about this in the same way as we do primary decomposition, so we just ignore the dimension of I as an R-module.

If I is prime, then the codimension of I is the dimension of R_I, that is, the length of the longest chain of primes contained in I. As $\dim I = \dim R/I$ and $\operatorname{codim} I = \dim R_I$, $\dim R \geq \dim I + \operatorname{codim} I$.

For general I, $\operatorname{codim} I = \min$ of $\operatorname{codim} P$ where P is a prime containing I.

If M is an R-module, then $\operatorname{codim} M = \operatorname{codim} \operatorname{Ann} M$.

Today: 0-dimensional Nötherian rings

If R has dimension zero, then all primes are maximal.

If R is a zero-dimensional domain, then 0 is a maximal ideal and so R is a field.

Recall: A ring R is Artinian iff it satisfies the descending chain condition on ideals.

Definition 8.2 (Composition Series)**.** *If M is an R-module, a composition series for M is $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n = 0$ with M_i/M_{i+1} a nonzero simple module (has no nontrivial submodules)*

The length of M is the smallest length of a composition series for M or ∞ if M has no finite composition series.

eg: the length of $\mathbb{Z}$ as a $\mathbb{Z}$-module if ∞.

eg: the length of $R = k[x]/x^2$ as an R-module is $R \supset (x) \supseteq 0$, so 2.

Proposition 8.2. *Let R be a ring and let M be an R-module. M has a finite composition series iff M is Artinian and Nötherian.*

In tis case, any filtration of submodules of M has length at most n and can be refined to a composition series.

Proof. Suppose that M is Artinian and Nötherian. Then by the ACC, M has a maximal proper submodule M_1, which has a maximal proper submodule M_2, etc. This gives a descending chain of proper submodules $M \supseteq M_1 \supseteq M_2 \supseteq \ldots$ where each M_i/M_{i+1} is simple. As M is Artinian, this chain must be finite, so some $M_n = 0$.

Suppose now that M has a finite composition series $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n = 0$. We first show that if $M' \subseteq M$ is a proper submodule, then the length of M' is less than the length of M.

Indeed, consider $M'_i = M' \cap M_i$. Then $M' = M'_0 \supseteq M'_1 \supseteq \ldots \supseteq M'_n = 0$. And $M'_i/M'_{i+1} = (M' \cap M_i)/(M' \cap M_{i+1}) = M'_i + M_{i+1}/M_{i+1} \subseteq M_i/M_{i+1}$. So M'_i/M'_{i+1} is either M_i/M_{i+1} and is simple, or it is zero. There must be at least one i for which $M'_i/M'_{i+1} = 0$, because otherwise we would get $M' \supseteq M_i$ for all i by descending induction, $M_n = 0 \subseteq M'$, so $M_i = M'_i + M_{i+1} \subseteq M'$ by induction. Then, $M' \supset M_0$, which is a contradiction.

This gives a filtration of $M' = M'_0 \supseteq M'_1 \supseteq \ldots \supseteq M'_n = 0$ where we leave out any repeated factor to get length $< n$. This is a composition series because successive quotients are simple. Thus, if we start with a composition series for M of minimal length, then M' has smaller length.

Now suppose that $M = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_k$ is a chain of submodules of M. By assumption, M has a composition series of length n. We will show that $k \leq n$. When $n = 0$, $M = 0$, so $k = 0$. Assume now that for $m < n$ a composition series of lenght m implies that all filtrations of submodules have length $\leq m$. Now N_1 is a proper submodule of M, and so has length $< length(M) \leq n$. So this means that $k - 1 < n$, so $k \leq n$.

Thus, every chain of submodules is finite, and so in particular every ascending chain and every descending chain is, so M is Artinian and Nötherian. $\square$

Corollary 8.3. *If M has length n, then every composition series of M has length n.*

Corollary 8.4. *If R is of finite length as an R-module, then R is Artinian and Nötherian.*

Theorem 8.5. *TFAE*

1. *R is Nötherian and all primes are maximal.*

2. *R is of finite length as an R-module.*

3. *R is Artinian.*

Proof. $1 \Rightarrow 2$: Let R be Nötherian with all primes maximal. Suppose that R is not of finite length as an R-module. Let I be an ideal maximal with respect to the property that R/I is not of finite length as an R-module. We claim that I is prime. If not, we can find $a, b \in R \setminus I$ with $ab \in I$. Then consider $0 \to R/(I : a) \to R/I \to R/(I, a) \to 0$. Both $(I : a)$ and (I, a) are strictly larger ideals, so $R/(I : a)$ and $R/(I, a)$ have finite length as R-modules. We can now get a finite composition series for R/I from the ones for $R/(I : a)$ and $R/(I, a)$, because length is additive in short exact sequences. This contradicts our assumption on I, so I is prime. As I is prime, it is maximal, so R/I is a field. Which has finite length. This contradiction means that I does not exist, so R has finite length as an R-module.

$2 \Rightarrow 3$: follows from the previous proposition.

$3 \Rightarrow 1$: Suppose that R is Artinian. We'll first show that 0 is a prime of finitely many maximal ideals. Since R is Artinian, we may choose from all ideals in R that are products of finitely many maximal ones a minimal one J. We want to show that $J = 0$. For each maximal ideals M, we must have $MJ = J$, so $J \subset M$, so J is contained in the intersection of all maximal ideals. $J^2 = J$

If J is nonzero, we can find an ideal I minimal wrt not annihilating J. Since $(IJ)J = IJ^2 = IJ \neq 0$, $IJ \subseteq I$. We must have $IJ = I$ by minimality of I. Also, $\exists f \in I$ with $fJ \neq 0$, so $I = (f)$. Since $IJ = I$, $\exists g \in J$ with $fg = f$, so $f(g - 1) = 0$, but $g - 1$ is in no maximal ideal, so it is a unit. Thus $f = 0$, and so $I = 0$ and $J = 0$.

The above is LEMMA: If R has finite length as an R-module, then $0 = M_1 \dots M_t$ where M_i are maximal.

Consider the R-module $V_s = M_1 \dots M_s / M_1 \dots M_{s+1}$ for $0 \leq s < t$. This is an R/M_{s+1}-module, and so a vector space. Subspaces of V_s correspond to ideals of R containing $M_1 \dots M_{s+1}$ and contained in $M_1 \dots M_s$. Since R is Artinian, V_s must be finite dimensional, so has a finite composition series. We now glue together the composition series for $R/M_1, M_1/M_1M_2, \dots$ to get a finite composition series for R.

So R has finite length as an R-modules, and is thus Nötherian. Now let P be a prime in R. Then $0 = M_1 \dots M_t \subseteq P$, so at least one $M_i \subseteq P$. But since M_i is maximal, $M_i = P$. Thus we have only a finite number of primes in R, each of which is maximal. $\square$

Corollary 8.6. *If R is Nötherian and dimension 0, then R is Artinian and there are only finitely many primes. Also, (0) is the product of powers of these primes.*

Corollary 8.7. *Let $V = V(I) \subseteq k^n$ be a variety over $k = \bar{k}$. TFAE*

1. *V is a finite set.*

2. *$k[x_1, \ldots, x_n]/\sqrt{I}$ is a finite dimensional k-vector sapce whose dimension is $|V|$.*

3. *$k[x_1, \ldots, x_n]/\sqrt{I}$ is Artinian.*

Proposition 8.8. *Let R be Nötherian and M a finitely generated R-module. TFAE*

1. *Some finite produt of maximal ideals $\prod_{i=1}^{s} P_i$ annihilates M.*

2. *All primes that contain the annihilator of M are maximal.*

3. *$R/\operatorname{Ann}(M)$ is Artinian.*

Proof. Suppose that $\prod P_i$ annihilates M. Let $P \supset \operatorname{Ann}(M)$. Then $P \supseteq \prod P_i$. So there exists i with $P_i \subseteq P$, and so $P_i = P$, as P_i is maximal.

R is Nötherian, so $R/\operatorname{Ann}(M)$ is, and every prime in $R/\operatorname{Ann}(M)$ is maximal, so by the theorem, $R/\operatorname{Ann}(M)$ is Artinian.

If $R/\operatorname{Ann}(M)$ is Artinian and Nötherian, then $0/\operatorname{Ann}(M) = \prod(P_i/\operatorname{Ann}(M))$, so $\prod P_i$ annihilate M. □

Recall: If $P \subseteq R$ is prime, $\operatorname{codim} P = \dim R_P$. (if (R, m) is local, $\operatorname{codim} m = \dim R$)

For general I, $\operatorname{codim} I = \min \operatorname{codim} P$ for $P \supset I$.

Goal: R Nötherian.

Theorem 8.9. *If $x_1, \ldots, x_c \in P$ and P is minimal among primes containing $x_1, \ldots, x_c$, then* $\operatorname{codim} P \leq c$.

This is a generalization of

Theorem 8.10 (Principle Ideal Theorem)**.** *If $x \in R$ and P is minimal among primes of R containing x, then* $\operatorname{codim} P \leq 1$.

Proof. We will show that every prime Q properly contained in P has codim 0.

Since P is minimal over x, all primes in R_P/x are maximal (since P_P/x is the only one) and R_P/x is Nötherian, so R_P/x is Artinian. Also, $x \notin Q$.

Look at the chain $Q_Q + (x), Q_Q^2 + (x) + \ldots$ in R_Q. It must stabilize, so $Q_Q^n + (x) = Q_Q^{n+1} + (x)$. So for any $f \in Q_Q^n$, we can write it as $f = ax + g$ with $g \in Q_Q^{n+1}$ and $a \in R_Q$.

So $ax \in Q_Q^n$, and thus $a \in Q_Q^n$, since x is not.

Thus, $Q_Q^n = xQ_Q^n + Q_Q^{n+1}$, so the finitely generated R_Q/Q_Q^{n+1}-module Q_Q^n/Q_Q^{n+1} satisfies $Q_Q^n/Q_Q^{n+1} = xQ_Q^n/Q_Q^{n+1}$.

The Idea WOULD HAVE BEEN appeal to Nakayama to get that $Q_Q^n = Q_Q^{n+1}$, and thus, $Q_Q^n = 0$ and thus $\operatorname{codim} Q = 0$. Look in book, and attempt to fill in details. □

Theorem 8.11. *If $x_1, \ldots, x_c \in R$ and P is minimal over primes containing $x_1, \ldots, x_c$, then* $\operatorname{codim} P \leq c$.

Proof. Localize at P to assume that R has a unique maximal ideal. Then since all primes in $R/(x_1, \ldots, x_c)$ are maximal, as P is the only one, we know that $\mathrm{Ann}(R/(x_1, \ldots, x_c)) \supset P^k$ for some k. Choose P_1 prime with $P_1 \subsetneq P$ with no primes between them. As R is Nötherian, this exists if $\operatorname{codim} P > 0$.

We will show that P_1 is minimal over an ideal generated by $c-1$ elements, which will, by induction that $\operatorname{codim} P_1 \leq c-1$, and so since P_1 was arbitrary, $\operatorname{codim} P \leq c$.

Since P is minimal over $(x_1, \ldots, x_c)$, there must be an x_i, say x_1, with $x_1 \notin P_1$. Thus P is minimal over (P_1, x_1), and so $\exists s$ with $P^s \subseteq (P_1, x_1)$.

So for $2 \leq j \leq c$, we can write $x_j^s = a_j x_1 + y_j$ with $y_j \in P_1$. Now we claim that P_1 is minimal over $(y_2, \ldots, y_c)$. Indeed, P is minimal over $(x_1, y_2, \ldots, y_c)$.

So $\operatorname{codim} P/(y_2, \ldots, y_c)$ in $R/(y_2, \ldots, y_c)$ is ≤ 1 by PIT. So $P_1/(y_2, \ldots, y_c)$ has codim 0, and so P_1 is minimal over $(y_2, \ldots, y_c)$. □

Corollary 8.12. $(x_1, \ldots, x_n) \subset k[x_1, \ldots, x_n]$ *has* $\operatorname{codim} = n$.

Corollary 8.13. *Prime ideals in a Nötherian ring satisfy the DCC with the length of a chain of ideals descending from a prime bounded by the number of generators of* P

Corollary 8.14 (Converse to PIT)**.** *Any prime* P *of* $\operatorname{codim} P = c$ *is minimal over an ideal generated by* c *elements.*

eg, $R = k[a, b, c, d]$ and $I = (ad - bc, ac - b^2, bd - c^2)$. $\dim R/I = 2$.

Corollary 8.15. *Any prime* P *of codim* c *is minimal over an ideal generated by* c *elements. (actually of codim* c*)*

Proof. The proof is by induction on c.

If $c = 0$, then P is minimal over 0, which has codim 0.

Now suppose that the corollary is true for smaller c and choose P_1 prime, maximal proper in P of codim $c-1$.

Then, by induction, P_1 is minimal over $(x_1, \ldots, x_{c-1})$ of codim $c-1$. Each prime Q_i minimal over $(x_1, \ldots, x_{c-1})$ has codimension $c-1$.

So $P \subsetneq Q_i$ for any Q_i minimal over $(x_1, \ldots, x_{c-1})$, so by prime avoidance, $P \not\subseteq \cup Q_i$. So we can find $x_c \in P \setminus \cup Q_i$. Then we must have P minimal over $(x_1, \ldots, x_c)$, as if $P' \subsetneq P$ contains it, then there exists P'' minimal over $(x_1, \ldots, x_{c-1})$ which has codim $c-1$, so $\operatorname{codim} P > c$, which is impossible.

Also, if Q is minimal over $(x_1, \ldots, x_c)$, then $\exists P'$ with $(x_1, \ldots, x_{c-1}) \subseteq P' \subsetneq Q$ and codim $P \geq c-1$. So $\operatorname{codim} Q \geq c$. By PIT $\operatorname{codim} Q = c$, so $\operatorname{codim}(x_1, \ldots, x_c) = c$. □

Corollary 8.16. *Let* (R, m) *be a local ring. Then* $\dim R = \min\{d | \exists x_1, \ldots, x_d \in m$ *with* $m^n \subset (x_1, \ldots, x_d)$ *for* $n >> 0\}$.

Proof. If $m^n \subset (x_1, \ldots, x_d) \subset m$, then m is minimal over $(x_1, \ldots, x_d)$. So $\operatorname{codim} m = \dim R \leq d$ by the PIT.

Conversely, it $d = \dim R = \operatorname{codim} m$, then by the converse to the PIT, $\exists x_1, \ldots, x_d$ with m minimal over $(x_1, \ldots, x_d)$. But $R/(x_1, \ldots, x_d)$ has only the

one prime ideal, we have that all elements of m are nilpotent module $(x_1, \ldots, x_d)$. So $\exists k$ such that $m^k \subset (x_1, \ldots, x_d)$, because the ring is Nötherian. (since if $m = (y_1, \ldots, y_s)$, $y_i^N = 0$ for all i, then $m^{sN} = 0$) $\square$

Definition 8.3 (System of Parameters)**.** *A system of parameters for $m \subset R$ with (R, m) local, is a sequence $x_1, \ldots, x_d$, $d = \dim R$ such that $m^n \subset (x_1, \ldots, x_d)$ for $n >> 0$.*

Parameters are a "local coordinate system" (up to finite ambiguity). eg, $k[x, y]_{(x,y)}$, parameters $(x^2 - y, y)$, so (up to the square) you are picking a horizontal line and a parabola to determine a point (determines 2, but that's finite ambiguity).

Recall: A family of varieties is $U \xrightarrow{\pi} B$. The fiber over b is "$\pi^{-1}(b)$" Algebraically, this is a map $R \to S$ with fiber over $P \subseteq R$ being $S \otimes R/P \simeq S/PS$.

We expect $\dim U \leq \dim B + \dim \pi^{-1}(b)$ for each b. Recall the blowup, $\pi^{-1}(0)$ has dimension 1 and $\dim B = \dim U = 2$ for the plane at the origin.

Theorem 8.17. *If $(R, m) \to (S, n)$ is a map of local rings, then $\dim S \leq \dim R + \dim S/mS$.*

Proof. Write $d = \dim R$, $e = \dim S/mS$. Then there exist $x_1, \ldots, x_d, s$ with $m^s \subseteq (x_1, \ldots, x_d)$ and $y_1, \ldots, y_e, t$ such that $n^t \subseteq (y_1, \ldots, y_e) + mS$.

Then, $n^{st} \subseteq ((y_1, \ldots, y_e) + mS)^s \subseteq m^s S + (y_1, \ldots, y_e) \subseteq (x_1, \ldots, x_d, y_1, \ldots, y_e)S$, so n is minimal over na ideal generated by $d + e$ elements, so $\operatorname{codim} n = \dim S \leq d + e = \dim R + \sim S/mS$. $\square$

Theorem 8.18. *If $(R, m) \to (S, n)$ is a map of local rings and S is flat over R, then $\dim S = \dim R + \dim S/mS$.*

We'll need the following:

Lemma 8.19. *If N is a flat R-module and $R \to T$ is any ring map, then $N \otimes_R T$ is flat over T.*

Lemma 8.20. *Suppose $\varphi : R \to S$ is a map of rings with S flat over R. If $P \supset P'$ are primes of R, and Q is a prime of S with $\varphi^{-1}(Q) = P$, then $\exists Q'$ of S contained in Q with $\varphi^{-1}(Q') = P'$.*

Corollary 8.21. *If (R, m) is a local ring, then $\dim \hat{R}_m = \dim R$.*

Proof. $\hat{R}_m$ is flat over R and $\hat{R}/m\hat{R} \simeq R/m$ is a field, so $\dim \hat{R}/m\hat{R} = 0$. $\square$

Theorem 8.22.

1. *If k is a field, then $\dim k[x_1, \ldots, x_n] = n$.*
2. *In general, $\dim R[x] = \dim R + 1$*
3. *If P is a prime of R, then $\exists$ a prime Q of $R[x]$ with $Q \cap R = P$, and for a maximal such ideal, $\dim R[x]_Q = 1 + \dim R_P$, so $\operatorname{codim}_{R[x]} Q = 1 + \operatorname{codim}_R P$.*

Proof. 1. Follows from 2 by induction on n.

2. If $P_1 \subset \ldots \subset P_d$ of R, we get $P_1R[x] \subset P_2R[x] \subset \ldots \subset P_dR[x] \subset P_dR[x] + (x)$. (using $PR[x] \cap R = P$ and if P is prime then $PR[x]$ is prime). So $\dim R[x] \geq \dim R + 1$.

   Conversely, if Q is a maximal ideal of $R[x]$, then Q is maximal among primes meeting $Q \cap R$, so by part 3, we get $\operatorname{codim} Q = 1 + \operatorname{codim} Q \cap R$, so $\dim R[x] \leq 1 + \dim R$.

3. We first prove the case where R is a field and $P = 0$. Then $Q \cap R = 0$ for any proper prime of $R[x]$, so we take Q to be any maximal ideal of $R[x]$. Then $\operatorname{codim} Q = 1 = 1 + \dim R$.

   In general, $PR[x]$ is a prime in $R[x]$ with $PR[x] \cap R = P$. Localize at P to assume that R is local and P is maximal. Let Q be a maximal ideal of $R[x]$ containing P. Then $Q \cap R = P$. So all the remains to be shown is that $\operatorname{codim} Q = 1 + \operatorname{codim} P$.

   If $P_0 \subset \ldots \subset P_d = P$ is a chain of primes in P, then $P_0R[x] \subset \ldots P_dR[x]$ is a chain in $R[x]$. Look at $Q/PR[x] \subseteq R[x]/PR[x] \simeq (R/P)[x]$, then $\operatorname{codim} Q/PR[x] = 1$. So $\operatorname{codim} Q \geq d + 1$.

   Then $\operatorname{codim} Q \leq \dim R_P + \dim R[x]_Q/PR[x]_Q = \dim R_p + 1 = \operatorname{codim} P + 1$. $\square$

Therefore, $\dim k[x_1, \ldots, x_n] = n$.

Definition 8.4 (Regular Local Ring)**.** *A ring (R, m) of dimension d is a regular local ring if m can be generated by d elements.*

If R is a regular local ring, then Nakayama says that $\dim_{R/m} m/m^2 = d$. Thus, every generating set for m has size d.

A generating set of size d is called a regular sequence of parameters.

Definition 8.5 (Regular Sequence)**.** *In general, a regular sequence is a sequence $x_1, \ldots, x_d$ such that $(x_1, \ldots, x_d)$ is proper and x_{i+1} is a nonzero-divisor on $R/(x_1, \ldots, x_i)$ for all i.*

Definition 8.6 (Cohen-Macaulay)**.** *A ring R is Cohen-Macaulay if there is a regular sequence of length $\dim R$.*

Goal: $\deg P_R + 1 = \dim R$.

Let $R = \oplus_{i \geq 0} R_i$ be a Nötherian graded ring with R_0 a field and R is generated as an R_0-algebra by R_1. This is sometimes called a standard-graded algebra.

This means $R = k[x_1, \ldots, x_n]/I$ for some n and homogeneous I.

Why? Because R is Nötherian, R_1 is a finite dimensional R_0-vector space. Then $k[x_1, \ldots, x_n]$ surjects onto R, so take I to be the kernel, which is homogeneous as this is a graded homomorphism of rings.

Definition 8.7 (Hilbert Function)**.** *The Hilbert function of R is $H_R(t) = \dim_k R_t$.*

In homework, we showed that there exists a polynomial $P_R(t)$ which is equal to the Hilbert Function for sufficiently large t.

If M is a graded R-module, then $H_M(t) = \dim_k M_t$. Again, it eventually will agree with a polynomial.

Lemma 8.23. *If $0 \to M' \to M \to M'' \to 0$ is a graded (ie, degree 0) short exact sequence of modules, then $H_M(t) = H_{M'}(t) + H_{M''}(t)$.*

Proof. The ses is the direct sum of ses $0 \to M'_d \to M_d \to M''_d \to 0$ of k-vector spaces, so additivity follows. □

Lemma 8.24. *If x is a nonzero divisor on R, homogeneous of degree 1, then $H_R(t) = H_R(t-1) + H_{R/x}(t)$ so $P_{R/x}(t) = P_R(t) - P_R(t-1)$ for all t, so $\deg P_R = \deg P_{R/x} + 1$.*

Proof. Consider the ses $0 \to R[-1] \xrightarrow{x} R \to R/x \to 0$ where $R[-1]$ is R with graded $R[-1]_n = R_{n-1}$. In general, $R[a]_b = R_{a+b}$.

So $H_R(t) = H_{R[-1]}(t) + H_{R/x}(t) = H_R(t-1) + H_{R/x}(t)$. □

Fact: If R is graded etcetera, then $\dim R = \max\{\operatorname{codim} Q | Q$ is a homogeneous prime$\}$.

Proposition 8.25. *If $\deg(x) > 0$ and x is a nonzerodivisor on R then $\dim R/x = \dim R - 1$.*

Proof. Since x is a nzd, x is not contained in any associated prime, so in particular, x does not lie in any minimal prime.

If $P_0 \subset \ldots \subset P_d$ is a chain of primes in R/x, that is, a chain of primes in R containing x, then $\exists$ prime $P \subsetneq P_0$ so $\dim R > \dim R/x$.

It remains to show that $\dim R/x \geq \dim R - 1$. Since R is graded and $\dim R < \infty$, there is a homogeneous prime Q with $\operatorname{codim} Q = \dim R$. Suppose that $\dim R/x = e < \dim R - 1$ with $d = \dim R$.

We know that $x \in Q$ since (Q, x) is proper (since Q, x are homogeneous) so contained in a maximal ideal. But Q is maximal. This menas that R_Q/x has $\dim \leq e$. So there are $x_1, \ldots, x_e \in Q$ qwith $Q_Q^n \subseteq (x_1, \ldots, x_e) + (x)$ for $n >> 0$. So $Q_Q^n \subseteq (x_1, \ldots, x_e, x)$, and so $\operatorname{codim} Q = \dim R_Q \leq e + 1$, so $d \leq e + 1$. □

Theorem 8.26. $\dim R = \deg P_R + 1$

Proof. The proof is by induction on dimension. If $\dim R = 0$, then R is Artinian.

So finite length ℓ as an R-module, so every filtration has length $\leq \ell$. If $R_{\ell+1} \neq 0$ $R \subset R_{>0} \subset R_{>1} \subset \ldots \subset R_{>\ell}$ is a filtration of length $\ell + 1$. If $R_{>j} = R_{>j+1}$ then $R_{j+1} = 0$, which implies that $R_n = 0$ for $n \geq j + 1$.

So this means that $R_n = 0$ for $n >> 0$, so $P_R(t) = 0$ which has degree -1 by convention.

We now assume that $\dim R > 0$ and that the theorem is true for smaller dimension. We first reduce to the case that $m = R_{>0}$ is not an associated prime. Since the zero divisors on R are the union of the associated primes, this will let us find a homogeneous nonzerodivisor (of degree 1)

Let $J = (0 :_R m^\infty) = \{f \in R | \exists k \text{ with } fm^k = 0\} = f \in R | \exists k \text{ with } fg = 0$ for all $g \in m^k\}$.

Let $R' = R/J$. First note that m is not associated to R', since if $(0 : x) = m$, then $x \in J$. Also note that $P_R = P_{R'}$ because $J_t = 0$ for $t >> 0$, because $J = (f_1, \ldots, f_s)$ for some s, where we can take f_i homogeneous.

Then there is a k such that $f_i m^k = 0$ for all i, then $J_t = 0$ for $t >> k + \max \dim f_i$. So $R_t = R'_t$ for $t >> 0$ so $P_R = P_{R'}$.

Also, $\dim R = \dim R'$, so since if $P_0 \subset \ldots \subset P_d$ is a chain of length $d = \dim R$ in R, then since $\dim R > 0$, $P_0 \neq m$, so we can find $x \in m \setminus P_0$ homogeneous, and then if $f \in J$, $fx^k = 0$ for $k >> 0$ so $fx^k \in P_0$, so $f \in P_0$. Thus $J \subseteq P_0$, so $\dim R' = \dim R$.

Thus, we assume that m is not an associated prime of R. So we can find $x \in R_1$ a nonzerodivisor on R. Then $\dim R/x = \deg P_{R/x} + 1$, by induction. And so, $\dim R = \dim R/x + 1$ and $\deg P_R = \deg P_{R/x} + 1$, so $\dim R = \deg P_R + 1$. $\square$

Fact: R graded, etc, then $\dim R = \max \operatorname{codim}$ of homogeneous Q. Why? Follows from $\dim k[x_1, \ldots, x_n]/I = \operatorname{tr} \deg_k R$ and all maximal ideals have the same codimension. This itself follows from Nöther Normalization.

Theorem 8.27 (Nöther Normalization)**.** *If $R = k[x_1, \ldots, x_n]/J$ then there exist $y_1, \ldots, y_d \in R$ such that $k[y_1, \ldots, y_d] \subseteq R$ and R is finite over S. (can take y_i to be homogeneous).*