Space Curves as Complete Intersections

Somnath Basu

Abstract

This is an expository account based mainly on an article by Jack Ohm titled *"Space curves as ideal-theoretic intersections"*. It also gives a proof of the fact that smooth space curves can be realized as set-theoretic complete intersections. The penultimate section proves the theorem of Cowsik and Nori : *Curves in affine n-space of characteristic p are set-theoretic complete intersection.*

Contents

1 Introduction

The question of how many polynomials are required to generate a given prime ideal $\mathfrak{p}$ in a polynomial ring $R = k[X_1, X_2, \ldots, X_n]$ over an algebraically closed field k, has been there for a long time. We should note the two extremal cases: the ht 1 primes in R, being an UFD, any prime ideal of R contains a prime element, are principal; the maximal ideals of R are generated by n polynomials by the correspondence of maximal ideals and points in k^n via Hilbert's Nullstellansatz. So, the very first example not covered by the earlier two cases is that of a ht 2 prime in $k[X_1, X_2, X_3]$, which, thought of geometrically, is the defining ideal of an irreducible (affine) space curve.

Macaulay showed that there exists such primes requiring arbitrary large number of generators. Since his examples are space curves with singularity at the origin, subsequent research has focussed on non-singular curves and in particular, on Serre's question of whether a non-singular irreducible space curve of genus $\leqslant 1$ is a complete intersection, i.e., whether the defining prime ideal can be generated by two elements.

We shall elaborate on the relationship between the Serre problem and minimal number of generators and subsequently applying the results obtained to space curves. This article is divided into seven main sections (§2-§8) with the ninth and last section containing results that will be needed as we proceed. One can always refer to it whenever the necessity arises.

2 The geometric setting

Fix an algebraically closed field k and $k[X] = k[X_1, X_2, \ldots, X_n]$. If $I \neq k[X]$, is an ideal then we shall write $k[x]$ to denote $k[X]/I$.

2.1 Affine Varieties

Since k is algebraically closed, it follows from Hilbert's Nullstellansatz that any maximal ideal of $k[X]$ is of the form $(X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_n - \alpha_n)$, where α_i's are in k. Thus, via this correspondence, we can think of maximal ideals as points in k^n. Moreover, if $\alpha \in k^n$ is a zero of I, then the corresponding maximal ideal $\mathfrak{m}_\alpha$ contains I and vice-versa. Hence, the word "point" can refer to α or $\mathfrak{m}_\alpha$, depending on the context. A **variety** in affine n-space k^n (denoted $\mathbf{A}_k^n$), will be taken to be the set $V(I)$ of maximal ideals of $k[X]$ containing a given radical ideal $I \neq k[X]$. Restricting to radical ideal ensures that $V(I) = V(J)$ implies $I = J$. This notion matches with the classical notion of a variety as the set of common zeroes of a collection of polynomials (the largest such collection defining the same zeroes is a radical ideal!) as we've identified the two notion of "points" earlier. The (reduced) ring $k[X]/I$ is called the **affine ring** of the variety $V(I)$; and two varieties, possibly over different affine spaces over k, are said to be **isomorphic** if their affine rings are k-isomorphic. The **dimension** of $V(I)$ is defined to be the Krull dimension of its affine ring, which is $n-\text{ht } I$.

2.2 Irreducible components

A variety $V(I)$ is called **irreducible** if it is not the union of two proper subvarieties, or equivalently, if I is prime. Every variety is the union of its maximal irreducible subvarieties, called its **irreducible components** and there are only finitely many such. A variety will be called **unmixed** if all its irreducible components have the same dimension, or equivalently ht $I_\mathfrak{p}$= ht I for any minimal prime $\mathfrak{p}$ of I. If $\mathfrak{m} \in V(I)$ then only the minimal primes of I contained in $\mathfrak{m}$ are preserved in passing to $k[X]_\mathfrak{m}$; so replacing I by $I_\mathfrak{m}$ basically amounts to ignoring those components of $V(I)$ which don't contain $\mathfrak{m}$. In particular, $\mathfrak{m}$ lies on a unique component of $V(I)$ iff $I_\mathfrak{m}$ is a prime, or equivalently iff $k[x]_\mathfrak{m}$ (which is $k[X]/I$ localized at $\mathfrak{m}$) is a domain, by the commutativity of localization and homomorphic images.

2.3 Simple points

A point $\mathfrak{m}$ of $V(I)$ is called **simple** (also called $non-singular$) on $V(I)$ if the local ring $k[x]_\mathfrak{m}$ is regular. Since a regular local ring is a domain (cf 2.1), by the above, a point of $V(I)$ is simple iff it lies on only one component and is simple on that component. The variety will be called **non-singular** if every point of $V(I)$ is simple, i.e. if the affine ring $k[x]$ is regular.

There is another classical definition of simple point; namely, a point $\mathfrak{m}_\alpha$ of $V(I)$ is called **simple** if the Jacobian matrix of $V(I)$ at α has rank equal to ht $I_\mathfrak{m}$. The Jacobian matrix is defined to be the $t \times n$ array whose $(i,j)th$ element is $(\frac{\partial f_i}{\partial x_j})$ evaluated at α, where $I = (f_1, f_2, \ldots, f_t)$. It is denoted by $\mathcal{J}(f_i;\alpha)$. It will be shown (later) that the rank of the matrix is independent of the generators chosen for I. So we shall use $\mathcal{J}(\alpha)$ (or $\mathcal{J}(I;\alpha)$) to denote the Jacobian matrix at α.

Assume that α is the origin and $\mathfrak{m}_\alpha = (X_1, X_2, \ldots, X_n)$, which we as well may by rewriting the polynomials of $k[X]$ as polynomials of $k[X-\alpha]$. Then the Jacobian is $\mathcal{J}(f_i;0) = (a_{ij})$ where $f_i = \sum_{j=0}^n a_{ij}X_j$ + higher degree monomials. So the rank of $\mathcal{J}(f_i;0)$ can thus be characterized as the maximal number of elements from among $f_1, f_2, \ldots, f_t$ s.t. they are linearly independent modulo $\mathfrak{m}^2$ over $k[X]/\mathfrak{m}(=k)$. If we localize at $\mathfrak{m}$ then any minimal generating set for $\bar{\mathfrak{m}} = \mathfrak{m}k[X]_\mathfrak{m}$ has the same size and equals the dimension of $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$ as a k-vector space by Nakayama's lemma. So, the rank is just the maximal number of elements from $I_\mathfrak{m}$ that is a part of some minimal generating set for $\mathfrak{m}k[X]_\mathfrak{m}$. We shall denote this number by $\nu(I)$.

2.4 The number $\nu(I)$

In this part we prove the equivalence of the two definitions of simple point.

Theorem 2.1. *Let $R, \mathfrak{m}$ be a local ring. Then $\mathfrak{p} = (a_1, a_2, \ldots, a_t)$ is a prime ideal of ht t iff $(0) < (a_1) < (a_1, a_2) < \cdots < (a_1, a_2, \ldots, a_t) = \mathfrak{p}$ is a chain of (necessarily saturated) prime ideals.*

The proof involves two lemmas:

Lemma 2.2. *Let R be a ring and (a) be a principal prime ideal of R. Then $(0) < (a)$ is a saturated chain of primes iff (i) ht (a)=1 and (ii) $\bigcap_{s=1}^{\infty} (a)^s = (0)$.*

Proof $\Rightarrow$: (i) is immediate. Also, R is a domain as (0) is prime. Let $xy \in \bigcap_{s=1}^{\infty} (a)^s$ for $x, y \in R$. If x or y, neither belongs to $\bigcap_{s=1}^{\infty} (a)^s$, then $x = a^s r_1$ and $y = a^t r_2$ for $r_1, r_2 \in R$ s.t. a does not divide r_1 or r_2. Since R is a domain, this would contradict that any power of a divides xy. Hence $\bigcap_{s=1}^{\infty} (a)^s$ is a prime ideal. Since ht (a) is 1, this implies (ii).

$\Leftarrow$: Since ht (a) is 1, there exists a prime ideal $\mathcal{Q}$ of R s.t. $\mathcal{Q} < (a)$. Take $q \in \mathcal{Q}$. Then $q = aq_1 \in \mathcal{Q}$. But $\mathcal{Q}$ is prime; this implies $q_1 \in \mathcal{Q}$. So $\mathcal{Q} = \mathcal{Q}(a)$. Repeating this we get : $\mathcal{Q} = \mathcal{Q}(a) = \cdots = \mathcal{Q}(a)^s = \cdots \subseteq \bigcap_{s=1}^{\infty} (a)^s = (0)$. Thus $\mathcal{Q} = (0)$. As $\mathcal{Q}$ was any prime of R lying below (a), the chain $(0) < (a)$ is saturated. □

Lemma 2.3. *Let $\mathfrak{p}$ be a prime ideal of a Noetherian ring R, $a \in \mathfrak{p}$ and $'$ denote the image of $\mathfrak{p}$ under the canonical map from R to $R/(a)$. Then ht $\mathfrak{p}' \geqslant$ ht $\mathfrak{p} - 1$.*

Proof Let ht $\mathfrak{p}'$ be s. Choose $b_1 \in \mathfrak{p}' \setminus \cup\{$minimal primes of $(0)\}$. Note that for $s = 1$, $\mathfrak{p}'$ is a minimal prime of (b_1). For $s \geqslant 1$ choose $b_2 \in \mathfrak{p}' \setminus \cup\{$minimal primes of $(b_1)\}$ and so on. This will give elements $b_1, b_2, \ldots, b_s$ in $R/(a)$ s.t. $\mathfrak{p}'$ is minimal over $(b_1, b_2, \ldots, b_s)$. Taking inverse images of the b_i's, we have $\mathfrak{p}$ to be minimal over an ideal generated by a and those s pre-images. Hence by Krull's PIT, ht $\mathfrak{p} \leqslant s + 1$. □

Proof of theorem : We proceed by induction on t. If $t = 1$ then by Krull's intersection theorem $\mathfrak{m}(\bigcap_{s=1}^{\infty} (\mathfrak{m})^s) = \bigcap_{s=1}^{\infty} (\mathfrak{m})^s$ and by Nakayama, $\bigcap_{s=1}^{\infty} (\mathfrak{m})^s$=(0). So, $\bigcap_{s=1}^{\infty} (a_1)^s = (0)$; and by 2.2 we are through. If t >1, let $R' = R/(a_1)$. Using 2.3 we have ht $\mathfrak{p}' \geqslant t - 1$. By PIT, $\mu(\mathfrak{p}') \geqslant$ ht $\mathfrak{p}'$ and $\mu(\mathfrak{p}') \leqslant t - 1$, thereby forcing equality. Using induction hypothesis and taking inverse images gives us the following chain of primes:

$$(a_1) < (a_1, a_2) < \cdots < (a_1, a_2, \ldots, a_t) = \mathfrak{p}.$$

By PIT, ht $(a_1) \leqslant 1$. If ht $(a_1) = 1$ then (0) is a prime by the case $t = 1$ of 2.2. So, we may assume that ht (a_1)=0. Choose r outside (a_1) but in all other ht 0 primes. We can certainly do so as R (being Noetherian) has finitely many minimal primes. Set $a_1^* = a_1 + ra_2$. Suppose (a_1^*) is contained in some minimal prime $\mathfrak{p}$ of R. Then $\mathfrak{p} \neq (a_1)$ and so $a_1 \in \mathfrak{p}$ as r does; a contradiction. Thus ht $(a_1^*) = 1$. Moreover, $(a_1, a_2, \ldots, a_t) = (a_1^*, a_2, \ldots, a_t)$; by the above deductions, (a_1^*) and (0) are both prime and so we're through. □

Note that 2.1 includes the fact that a regular local ring is a domain.

Definition 2.4. $\nu(I)$ = sup {s | I contains s elements which form a part of a minimal generating set for $\mathfrak{m}$}, where $R, \mathfrak{m}$ is local ring.

Theorem 2.5. *Let $R, \mathfrak{m}$ be a regular local ring and let $I \neq R$ be an ideal of R. Then $\nu(I) \leqslant htI$ and equality holds iff R/I is regular. Moreover, when equality holds, I is prime and $\nu(I) = htI = \mu(I)$ and any minimal generating set for I can be extended to a minimal generating set for $\mathfrak{m}$.*

Proof Put $\nu = \nu(I)$. Then there exists $a_1, a_2, \ldots, a_\nu \in I$ and $b_{\nu+1}, \ldots, b_t \in \mathfrak{m}$ s.t. $a_1, a_2, \ldots, a_\nu$, $b_{\nu+1}, \ldots, b_t$ is a minimal generating set for $\mathfrak{m}$. Since R is regular, ht $\mathfrak{m} = t$. So, by 2.1 $(0) < (a_1) < (a_1, a_2) < \cdots < (a_1, a_2, \ldots, a_\nu) < (a_1, a_2, \ldots, a_\nu, b_{\nu+1}) < \cdots < (a_1, a_2, \ldots, a_\nu, b_{\nu+1}, \ldots, b_t) = \mathfrak{m}$ is a saturated chain of primes. In particular, $(0) < (a_1) < (a_1, a_2) < \cdots < (a_1, a_2, \ldots, a_\nu)$ is a saturated chain of primes in I. Thus ht $I \geqslant \nu$. If ht $I = \nu$, then by Krull's PIT : $\nu \geqslant \mu(I) \geqslant$ ht $I = \nu$ and I must equal $(a_1, a_2, \ldots, a_\nu)$. So, I is prime and $\nu(I) = \mu(I) =$ ht I. Also, $t - \nu \geqslant \mu(\mathfrak{m}/I) \geqslant$ ht $\mathfrak{m}/I \geqslant t - \nu$; the first inequality following from definition, the second by PIT and the third by 2.1 applied to R/I.

To prove the converse, it suffices to show that if R/I is regular then any minimal generating set for I can be extended to a minimal generating set for $\mathfrak{m}$; for then, $\mu(I) \leqslant \nu(I)$ and hence ht $I = \nu(I)$. Let $a_1, a_2, \ldots, a_s$ and $b'_1, b'_2, \ldots, b'_t$ be minimal generating sets for I and $\mathfrak{m}/I$ respectively. Then $a_1, a_2, \ldots, a_s, b_1, b_2, \ldots, b_t$ generate $\mathfrak{m}$ where b_i's are (any chosen) pre-images of b'_i's. It is clear that any minimal generating set $\mathcal{S}$ for $\mathfrak{m}$ among this set of generators must contain the b_i's. So, assume, with a relabelling if necessary, that $\mathcal{S} = \{a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_t\}$, $r \leqslant s$. But the following chain of ideals has its first $r+1$ members prime (by 2.1 applied to (R, m)) and its last $t+1$ members prime (by 2.1 applied to $(R/I, m/I)$) :

$$(0) < (a_1) < \cdots < (a_1, a_2, \ldots, a_r) \subseteq I < I + (b_1) < I + (b_1, b_2) < \cdots < I + (b_1, b_2, \ldots, b_t) = \mathfrak{m}.$$

Since ht $\mathfrak{m} = \mu(\mathfrak{m}) = t + r$, $I = (a_1, a_2, \ldots, a_r)$ implying $r = s$. □

Note that since $\nu(I)$, in the discussion of §2.3, was seen to be the rank of the Jacobian matrix, the above theorem proves the equivalence of the two notions of simple points.

Corollary 2.6. *If $I \neq R$ is an ideal s.t R/I is regular, then I is a radical ideal and is locally a complete intersection ideal (i.e. ht $I_\mathfrak{p} = \mu(I_\mathfrak{p})$) at all primes $\mathfrak{p} \in V(I)$.*

Before proving it let us note that R regular implies that $R_\mathfrak{p}$ is also regular for any prime ideal $\mathfrak{p}$. We shall assume this fact.??

Proof R/I is regular implies $(R/I)_\mathfrak{p}$ is regular local $\forall$ $\mathfrak{p} \supseteq I$. Thus, 2.5 implies ht $I_\mathfrak{p} = \mu(I_\mathfrak{p})$ and that $I_\mathfrak{p}$ is prime. We show that R/I is reduced (equivalently I is radical). Let x be a nilpotent element of R/I. Set $M = (x)$. Observe that $M_\mathfrak{p} = 0$ since $(R/I)_\mathfrak{p}$ is a domain and $\bar{x}$, the image of x in $(R/I)_\mathfrak{p}$, is nilpotent; hence zero. This is true for $\mathfrak{p} \in \mathrm{Spec}R/I$. So $M = 0$ and R/I is reduced. □

It is interesting to note that the converse to 2.6 is false : *The prime ideal $I = (Y^2 - X^3)$ in $k[X, Y]$, k alg. closed field, is locally a complete intersection at primes $\supseteq I$, but $k[X, Y]/I$ is not regular.*

Let $\mathfrak{m} = \mathfrak{m}_\alpha$ be a maximal ideal containing I. This means that $\alpha = (\alpha_1, \alpha_2) \in \mathbf{A}^2_k$ is a zero of $Y^2 - X^3$. We already have ht $I = 1$ and $\mu(I) = 1$. Hence equality prevails in $1 =$ ht $I =\leqslant$ ht $I_\mathfrak{m} \leqslant \mu(I_\mathfrak{m}) \leqslant \mu(I) = 1$. Thus I is a local c.i. But $k[X, Y]/I$ is not regular as for any maximal ideal $\mathfrak{m} \supset I$ other that (X, Y) has $\mu((\mathfrak{m}/I)_\mathfrak{m}) = 2$ (can be seen by assuming the contrary and a simple calculation) whereas ht $\mathfrak{m}/I)_\mathfrak{m} = 1$. Hence $k[X, Y]/I$ is not regular.

2.5 Complete Intersections

An ideal I of a Noetherian ring R is called a **complete intersection** if $\mu(I) =$ ht I. Analogously, a variety $V(I)$ will be called a complete intersection (more specifically, an ideal-theoretic complete intersection) if I is a c.i. ideal. By a **space-curve** C we mean 1-dimensional, unmixed variety in $\mathbf{A}_k^3$. It is a c.i. if $\mu(I_C) = \text{ht } I_C$, where I_C is the defining ideal of the curve.

Recall that a surface f in $\mathbf{A}_k^3$ is a 2-dimensional unmixed variety or equivalently a variety defined by a polynomial $f \in k[X_1, X_2, X_3]$ s.t. f has no repeated factors in its irreducible decomposition. This is the same as requiring (f) to be radical ideal. A space-curve C will be called a **set-theoretic complete intersection** of surfaces (f) and (g) if the intersection of the set of zeroes of f and g is that of I_C, i.e., if $V(I_C) = V((f)) \cap V((g)) = V((f, g))$ or equivalently if $I = \sqrt{(f, g)}$. It is clear that if C is a complete intersection then it is a set-theoretic complete intersection. It is also known that a sufficient condition for the two surfaces (f) and (g) to define C as a set-theoretic c.i. is that both should be transversal at every point of C.

3 A local-global principle

Let $I \neq R$ be a f.g. regular ideal of ring R. Recall that an ideal is called *regular* if it contains a non-zero divisor of R. The Förster-Swan theorem tells us how to use a collection of local bounds $\{\mu(I_\mathfrak{p})\}$ to obtain a bound for $\mu(I)$. We shall work out some of the details of this and show how it can be used to prove that the ideal of a non-singular space curve is generated by at most 3 elements.

3.1 Projective dimension

We shall defer the proofs of the results needed regarding the same to §8. The reader is asked to refer to that whenever there is a need during the discussion. Simply put, $d(M) = 1$ for a f.g. R-module M means that there is an exact sequence of R-modules of the form $0 \to P_1 \to P_0 \to M \to 0$ with P_0, P_1 both f.g. projective and M itself not projective. This is more or less what is required regarding projective dimension in theorem 3.1.

3.2 Ext_R^1

An exact sequence $E : 0 \to A \to B \to C \to 0$ of R-modules is called an **extension** of A by C. Two such extensions E and E' are said to be equivalent if there exists an isomorphism of the middle terms B and B' such that the following diagram commutes:

$$\begin{array}{lccccccccc} E: & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & \downarrow id & & \downarrow \wr\| & & \downarrow id & & \\ E': & 0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

The set of equivalence classes of such extensions can be given an R-module structure and is denoted by $\text{Ext}_R^1(C, A)$. Given two extensions E and E' of A by C form $E \oplus E'$:

$$0 \to A \oplus A \xrightarrow{f} B \oplus B' \xrightarrow{g} C \oplus C \to 0$$

Let $d : C \to C \oplus C$ be the diagonal map. Then via pull-back, we have an exact sequence :

$$0 \to A \oplus A \xrightarrow{h} X' \to C \to 0$$

Here $X' = ker(-g, d) : B \oplus B' \oplus C \to C \oplus C$. Similarly, let $s : A \oplus A \to A$ be given by $s(a, a') = a + a'$. Then by push-out, we have :

$$0 \to A \to B'' \to C \to 0$$

Here $B'' = coker(-h, s) : A \oplus A \to X' \oplus A$. This defines the (well-defined!) addition. For multiplication, observe that for $r \in R$, $r : A \to A$ (multiplication by r) induces a map of exact sequences $0 \to A \to B' \to C \to 0$ via push-out. This makes Ext^1_R into an R-module.
The Ext defined in this way is known as **Yoneda's Ext**. One can define Ext^n_R for higher n and prove that the alternative notion of Ext as the left-derived functor of the right-exact functor $\text{Hom}_R(\_\,, N)$ are the same. A good reference for this is [1] pgs.652-654.

Properties

1. Given an extension $E : 0 \to A \to B \to C \to 0$ and an R-module N, there exists an exact sequence of R-modules (via the alternative defn. of Ext):

$$0 \to \text{Hom}_R(C, N) \to \text{Hom}_R(B, N) \to \text{Hom}_R(A, N) \xrightarrow{\phi} \text{Ext}^1_R(C, N) \to \text{Ext}^1_R(B, N) \to \text{Ext}^1_R(A, N) \to \cdots \to \text{Ext}^i_R(B, N) \to \text{Ext}^i_R(A, N) \to \text{Ext}^{i+1}_R(C, N) \to \cdots$$

   Note that $\text{Ext}^1_R(C, A)$=0 iff every extension splits. So, if C is projective, $\text{Ext}^1_R(C, A)$=0. Assuming $A = N = R$ in E, we have $\phi(1) = [E]$. If B is projective $\text{Ext}^1_R(B, R) = 0$; thus ϕ is surjective and $[E]$ generates $\text{Ext}^1_R(C, R)$.

2. If $E : 0 \to K \to P \to C \to 0$ with P projective, then $0 \to Hom_R(C, N) \to Hom_R(P, N) \to Hom_R(K, N) \to Ext^1_R(C, N) \to 0$ is exact. Localizing at a mult. closed set S of R and localizing E at S and then taking the exact sequence gives the following resp.:

$$0 \to \text{Hom}_R(C, N)_S \to \text{Hom}_R(P, N)_S \to \text{Hom}_R(K, N)_S \to \text{Ext}^1_R(C, N)_S \to 0$$

$$0 \to \text{Hom}_{R_S}(C_S, N_S) \to \text{Hom}_{R_S}(P_S, N_S) \to \text{Hom}_{R_S}(K_S, N_S) \to \text{Ext}^1_{R_S}(C_S, N_S) \to 0$$

   If P is f.g., then P is finitely presented (f.p.). Assume K is also f.p. Then $\text{Hom}_{R_S}(P_S, N_S) \cong \text{Hom}_R(P, N)_S$ and $\text{Hom}_{R_S}(K_S, N_S) \cong \text{Hom}_R(K, N)_S$. Then $\text{Ext}^1_{R_S}(C_S, N_S) \cong \text{Ext}^1_R(C, N)_S$.

   As we shall later that if $d(C) = 1$, i.e. projective dimension is 1, then K (as above) can be chosen to be f.g. free, in which case $\text{Hom}_R(K, R)$ and hence $\text{Ext}^1_R(C, R)$ is finitely generated.

3. If I is an ideal of R s.t. $d(I)$=1, then $V(Ann\ \text{Ext}^1_R(I, R)) \subset V(I)$. For if $\mathfrak{p} \in \text{Spec}R$, then $\mathfrak{p} \not\supset I \Rightarrow I_\mathfrak{p} = R_\mathfrak{p} \Rightarrow \text{Ext}^1_{R_\mathfrak{p}}(I_\mathfrak{p}, R_\mathfrak{p}) = 0$. Because $d(I) = 1$, by (2) above, $\text{Ext}^1_R(I, R)_\mathfrak{p} = 0$. Since $\text{Ext}^1_R(I, R)$ is f.g., $\exists s \in R \setminus \mathfrak{p}$ s.t. s annihilates $\text{Ext}^1_R(I, R)$. So, $\mathfrak{p} \not\supset Ann\ \text{Ext}^1_R(I, R)$.

4. $\text{Ext}^1_R(C, A_1 \oplus A_2) \cong \text{Ext}^1_R(C, A_1) \oplus \text{Ext}^1_R(C, A_2)$. In particular, if $d(C) = 1$ then $\text{Ext}^1_R(C, R) \neq 0$. If not, then let $0 \to R^t \to P \to C \to 0$ be a finite projective resolution of C. Then $\text{Ext}^1_R(C, R^t) = \bigoplus_{i=1}^{t} \text{Ext}^1_R(C, R)$=0. Thus, $P \cong R^t \oplus C$ with P projective means C is, contradicting $d(C) = 1$.

3.3 The theorem of Serre-Murthy

Theorem 3.1. *Suppose M is a f.g. R-module with d(M)=1. Then the following positive integers are equal:*

(i) inf $\{t \mid \exists$ *an exact sequence* $0 \to R^t \to P \to M \to 0$ *with* P *f.g. proj.*$\}$
(ii) inf $\{\mu(P_1) \mid \exists$ *an exact sequence* $0 \to P_1 \to P_0 \to M \to 0$ *with* P_0, P_1 *f.g. proj.*$\}$
(iii) $\mu(Ext^1_R(M, R))$

Proof : (i) $\iff$ (ii) : The integer in (ii) is at most that in (i). So, take t to be the integer in (ii) and $0 \to P_1 \to P_0 \to M \to 0$ s.t. $\mu(P_1) = t$. Then P_1 admits a direct summand Q s.t. $P_1 \oplus Q \cong R^t$. This gives an exact sequence $0 \to R^t \to P_0 \oplus Q \to M \to 0$ with $P_0 \oplus Q$ f.g. projective. So we're done.
(i) $\iff$ (iii) : If there is an exact sequence $0 \to R^t \to P \to M \to 0$ with t as in (i), then we have an exact sequence $\cdots \to \mathrm{Hom}_R(R^t, R) \to \mathrm{Ext}^1_R(M, R) \to 0 \to \cdots$. So, $\mu(\mathrm{Ext}^1_R(M, R)) \leqslant t$ as $\mathrm{Hom}_R(R^t, R)$ surjects onto $(\mathrm{Ext}^1_R(M, R))$.
Conversely, suppose that $\mu(\mathrm{Ext}^1_R(M, R)) \leqslant t$. Note that $t \geqslant 1$ as $d(M) = 1$ implies $\mathrm{Ext}^1_R(M, R) \neq 0$ (by property 4 in §3.2). It suffices to show that there is an exact sequence $0 \to R^s \to Q \to M \to 0$ with Q f.g. projective. Let $[E_1], [E_2], \ldots, [E_t]$ generate $\mathrm{Ext}^1_R(M, R)$ and let E_1 be $0 \to R \to L \xrightarrow{g} M \to 0$. This gives the long exact sequence :

$$\cdots \to \mathrm{Hom}_R(R, R) \xrightarrow{\phi} \mathrm{Ext}^1_R(M, R) \xrightarrow{\psi} \mathrm{Ext}^1_R(L, R) \to 0 \text{ where } \phi(1) = [E_1]$$

Hence $\psi([E_1]) = 0$ and either (i) $t = 1$, $\mathrm{Ext}^1_R(L, R) = 0$ or (ii) $t > 1$ and $\mathrm{Ext}^1_R(L, R)$ is generated by the $t - 1$ elements $\psi([E_2]), \ldots, \psi([E_t])$. We proceed by induction on t. Note that $d(L) \leqslant 1$ as $d(M) = 1$. So, if $d(L) = 0$ then L is f.g. projective and E_1 is the required sequence. Also if $t = 1$ then $\mathrm{Ext}^1_R(L, R) = 0$ implying l is f.g. projective and again E_1 suffices. So, assume $t > 1$ and $d(L) = 1$ and $\mathrm{Ext}^1_R(L, R)$ is generated by $t - 1$ elements. By induction hypothesis there is an exact sequence $0 \to R^s \to Q \xrightarrow{f} L \to 0$ with Q f.g. projective and $s \leqslant t-1$. Taking K to be $ker(f \circ g)$, using Snake's lemma and verifying the necessary exactness, we have the following exact commutative diagram :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & R^s & & R^s & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \dashrightarrow & K & \dashrightarrow & Q & \xrightarrow{f\circ g} & M & \dashrightarrow & 0 \\
 & & \downarrow & & \downarrow f & & \| & & \\
0 & \longrightarrow & R & \longrightarrow & L & \xrightarrow{g} & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

It follows (from above) that $K \cong R^s \oplus R$ and so we have the required sequence for M. □

Corollary 3.2. *Let* I *be a regular ideal of* R*,* $d(I) = 1$ *and f.g.* R*-projectives are free. Then* $\mu(I) = \mu(Ext^1_R(I, R)) + 1$.

Proof : Since I is regular, $I \notin \mathfrak{p}$ for any minimal prime $\mathfrak{p}$ of R. Thus, $I_{\mathfrak{p}} = R_{\mathfrak{p}}$ for such a prime and rank$I$ is 1. Localizing the exact sequence $0 \to R^t \to R^s \to I \to 0$ at $\mathfrak{p}$ (ht $\mathfrak{p} = 0$) and adding ranks we get $s = t + 1$. If $t = \mu(\mathrm{Ext}^1_R(I, R))$ then $\mu(I) \leqslant s = \mu(\mathrm{Ext}^1_R(I, R)) + 1$. On the other hand if $s = \mu(I)$ then the kernel K of $R^s \to I$ is f.g. projective by Schanuel's lemma and hence free; so,

$\mu(I) = s \geqslant \mu(K) + 1 \geqslant \mu(\text{ Ext}^1_R(I,R)) + 1$. Hence equality prevails. □

Keeping in mind the case of the polynomial ring over fields and looking forward to §4.3 , we see that the hypothesis of the following corollary implies $d(I) = 1$.

Corollary 3.3. *Suppose I is a ht 2 unmixed ideal of $R = k[X_1, X_2, \ldots, X_n]$, k a field. If I is locally a c.i. at every prime containing I, then I is a c.i. iff $Ext^1_R(I,R)$ is cyclic.*

Proof : Immediate from previous remark and cor 3.2. □

Theorem 3.1 generalizes to any f.g. R-module M s.t. $d(M) < \infty$ but since it will not be relevant for our purpose we state it without proof. It can be proved by induction on $d(M)$.

Theorem 3.4. *Suppose $d(M) = n \geqslant 1$. Then the following positive integers are equal :*
(i) inf $\{t \mid \exists$ an exact sequence $0 \to R^t \to P_{n-1} \to \cdots \to P_0 \to M \to 0$ with P_i's f.g. proj.$\}$
(ii) inf $\{\mu(P_n) \mid \exists$ an exact sequence $0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$ with P_i's f.g. proj.$\}$
(iii) $\mu(Ext^n_R(M,R))$

3.4 The Förster-Swan theorem

For a f.g. module N, we are interested in finding $\mu(N)$. Roughly speaking, the theorem states that if $\mu(N_\mathfrak{p}) \leqslant \beta$ for all $\mathfrak{p} \in \text{Spec}R$ and $\alpha = \text{coht } (Ann\ N)$, then $\mu(N) \leqslant \beta + \alpha$.
To state the general theorem we need some terminology :
A *j-radical* is the intersection of maximal ideals.
A *j-prime* is a prime ideal which is *j-radical.*
A ring R will be called *j-Noetherian* if it satisfies the a.c.c on *j-radical* ideals. It is also said to have *Noetherian j-spectrum.*
The *j-dimension* of R is the maximal length of chain of *j-primes.*
Analogously, *j-coht (I)* is the maximal length of *j-primes* ascending from I.
$V_j(I)$ is the set of *j-primes* containing I.
Finally, for notational convenience denote $\mu^*(\mathfrak{p}, N)$ to be $\mu(N_\mathfrak{p}) + j\text{−coht } (\mathfrak{p})$ where $\mathfrak{p} \in \text{Spec}R$ and N, a f.g. R-module.

Förster-Swan Theorem : *Suppose R is j-Noetherian and $N \neq 0$ is a f.g. R-module and R is of finite j-dimension. Then $\mu(N) \leqslant sup\{\mu^*(\mathfrak{p}, N) \mid \mathfrak{p} \in V_j(Ann\ N)\}$.*

We shall apply this in §3.6. A very good source for a proof of this is Swan's original paper.

3.5 Rank of a module

For a f.g. R-module define rank $N = \inf\{\mu(N_\mathfrak{p}) \mid \text{ht } \mathfrak{p} = 0, \mathfrak{p} \in \text{Spec}R\}$. Since μ doesn't increase under localization and $N_\mathfrak{p} = (N_{\mathfrak{p}'})_{\mathfrak{p}R_{\mathfrak{p}'}}$ where $\mathfrak{p} \subseteq \mathfrak{p}'$, we have $\mu(N_\mathfrak{p}) \leqslant \mu(N_{\mathfrak{p}'})$. So, rank $N = \inf\{\mu(N_\mathfrak{p}) \mid \mathfrak{p} \in \text{Spec}R\}$ as well. After this, when we say a f.g. R-module of rk n we mean that $\mu(M_\mathfrak{p}) = n$ for any $\mathfrak{p} \in \text{Spec}R$.
If one has a s.e.s of the form $0 \to R^t \to P \to M \to 0$ with P f.g. projective, then by 9.8 $M_\mathfrak{p}$ is free for a ht 0 prime $\mathfrak{p}$ and we have $P_\mathfrak{p} \cong R^t \oplus M_\mathfrak{p}$. Adding ranks (of free modules) we get : $\mu(M_\mathfrak{p}) + t = \mu(P_\mathfrak{p})$. Thus both $\mu(P_\mathfrak{p})$ and $\mu(M_\mathfrak{p})$ attain its minimum at the same ht 0 primes. So, we have rk $p = t+$rk M where t can be chosen to be the integer in 3.1(i). Denote t as per 3.1(i) by $\mu_1(M)$.

Now take $0 \to Q \to R^s \to M \to 0$ with $s = \mu(M)$ and Q f.g. projective. Then $s = \mu(M_\mathfrak{p}) + \mu(Q_\mathfrak{p})$ and $\mu(M) \geqslant$ rk $Q+$ rk M. If Q is free, rk $Q = \mu(Q) \geqslant \mu_1(M)$, giving $\mu(M) \geqslant$ rk $M + \mu_1(M)$. Putting it all together : If $d(M) = 1$ and f.g. R-projectives are free, then $\mu(M) =$ rk $M + \mu_1(M)$.

Lemma 3.5. *Let R be a reduced ring and N a f.g. R-module. Then rk $N = \mu(N)$ iff N is free.*

Proof : The "only if" part is trivial. So suppose rk $N = \mu(N) = t$. Then $\mu(N_\mathfrak{p}) = t$ $\forall \mathfrak{p} \in \text{Spec}R$. Let $x_1, x_2, \ldots, x_t$ generate N and suppose $\sum_{i=1}^{t} r_i x_i = 0$. Since $\mu(N_\mathfrak{p}) = t$ and this relation holds locally, none of the r_i's localize to an unit, i.e. $r_i \in \bigcap_{\mathfrak{p} \in SpecR} = 0$, $\forall$ $i = 1, 2, \ldots, t$. □

3.6 A bound for $\mu(M)$

Theorem 3.6. *Let R be a ring having Noetherian j-spectrum and finite j-dimension, M be a f.g. R-module s.t. $d(M) = 1$. Denote $Ann(Ext^1_R(M, R))$ by A_1. Then $\mu_1(M) \leqslant sup\{\mu^*(\mathfrak{p}, M) | \mathfrak{p} \in V_j(A_1)\} - rkM$. If in addition, f.g. R-projectives are free, then $\mu(M) \leqslant sup\{\mu^*(\mathfrak{p}, M) | \mathfrak{p} \in V_j(A_1)\}$.*

Proof : Since f.g. projectives over local rings are free, we have $\mu(M_\mathfrak{p}) = \mu_1(M_\mathfrak{p})$+rk $M_\mathfrak{p}$ $\forall \mathfrak{p} \in V_j(A_1)$ by §3.5. Then $\mu^*(\mathfrak{p}, M) = \mu(M_\mathfrak{p}) + j-$coht $\mathfrak{p} = \mu(\text{Ext}^1_R(M_\mathfrak{p}, R_\mathfrak{p})) + j-$coht $\mathfrak{p}$+rk $M_\mathfrak{p} = \mu^*(\mathfrak{p}$,$\text{Ext}^1_R(M, R))$+rk $M_\mathfrak{p} \geqslant \mu^*(\mathfrak{p}$,$\text{Ext}^1_R(M, R))$+rk M. By Förster-Swan, $\mu_1(M) \leqslant \mu(\text{Ext}^R_1(M, R)) \leqslant$ sup$\{\mu^*(\mathfrak{p}$,$\text{Ext}^1_R(M, R) | \mathfrak{p} \in V_j(A_1)\} \leqslant$ sup$\{\mu^*(\mathfrak{p}, M) | \mathfrak{p} \in V_j(A_1)\}$−rk M. If f.g. R-projectives are free, then by §3.5 $\mu(M) = \mu_1(M)$+rk M. Hence, $\mu(M) \leqslant$ sup$\{\mu^*(\mathfrak{p}, M) | \mathfrak{p} \in V_j(A_1)\}$. □

Since we are concerned with $R = k[X_1, X_2, \ldots, X_n]$ and $M = I$, a regular ideal, we rephrase the theorem for this case :

Corollary 3.7. *Let R be j-Noetherian having finite j-dimension and let I be a regular ideal s.t. $d(I) = 1$. If β =$sup\{\mu^*(\mathfrak{p}, I) | \mathfrak{p} \in V_j(I)\}$, then $\exists$ a s.e.s $0 \to R^{\beta-1} \to P \to I \to 0$ with P projective of constant rank β. If f.g. R-projectives (of const. rank β) are free, then $\mu(I) \leqslant \beta$.*

Proof : Observe I, being regular,is locally a free $R_\mathfrak{p}$-module for $\mathfrak{p}$ of ht 0 of rank 1. From the proof of 3.6 $\mu(\text{Ext}^1_R(I, R)) \leqslant \beta - 1$. Thus $\exists$ a s.e.s $0 \to R^{\beta-1} \to P \to I \to 0$. Adding up local ranks we find that P is a projective of constant rank β. Further, if P is free, then clearly $\mu(I) \leqslant \beta$. □

Now consider the case of a ht 2 unmixed ideal I s.t. $\mu(I_\mathfrak{p}) = 2$ for $\mathfrak{p} \in V(I)$ I of $R = k[X_1, X_2, X_3]$ s.t. $d(I) = 1$. Notice that sup$\{\mu^*(\mathfrak{p}, I) \mid \mathfrak{p} \in V_j(I)\} \leqslant 3$. By the Quillen-Suslin theorem f.g. $k[X_1, X_2, \ldots, X_n]$-projectives are free. Thus we see that for a non-singular space curve $\mu(I) \leqslant 3$. This bound is the best possible.

4 When is $d(I) = 1$?

Throughout this section, R will denote a Noetherian ring unless stated otherwise and I an ideal of R s.t. $I \neq R$. The main result that we will prove (in 4.4) is about some general criteria for when $d(I) = 1$. One can skip 4.1 for the present purpose but this will be used later.

4.1 Invertible ideals

A regular ideal I of an arbitrary ring R is called **invertible** if I is a f.g. ideal which is locally principal. Since I is regular, locally principal is the same thing as locally free of rank 1. Since I is f.g., it is projective of constant rank 1. Conversely, if I, an ideal, is a f.g. R-projective of constant rank 1, then it is locally free of rank 1. Thus in view of this, we can also define an **invertible** ideal as a f.g. projective regular ideal of constant rank 1.
We have the following related proposition on Noetherian rings R :

Proposition 4.1. *Any f.g. R-projective P of constant rank 1 is isomorphic to an invertible ideal of R.*

Proof: Let $S =$ set of regular elements of R. So the complement of S is the union of finitely many minimal primes $\mathfrak{p}_i$'s $(i = 1, 2, \ldots, n)$ of R and on passing to R_S, the only maximal ideals are $\mathfrak{p}_i R_S$, $i = 1, 2, \ldots, n$. Notice P_S is still a f.g. projective of constant rank 1. Assuming, for the time being, that P_S is R_S-free, we have $(P_S)_{\mathfrak{p}_i R_S} = ({R_S}^t)_{\mathfrak{p}_i R_S}$. But $(P_S)_{\mathfrak{p}_i R_S} \cong P_{\mathfrak{p}_i} \cong R_{\mathfrak{p}_i}$. Thus $t = 1$ and $P_S = R_S$; but the natural map $P \to P_S$ is injective as P is torsion-free. and P is isomorphic to a submodule of R_S. Since P is f.g. $\exists s \in S$ s.t. $sP \subseteq R$, whence sP is an ideal isomorphic to P by regularity of P. It remains to show that an ideal I of a Noetherian ring R which is locally free of constant rank 1 is regular. Now $0 = Ann_{R_\mathfrak{p}}(I_\mathfrak{p}) = Ann_R(I)_\mathfrak{p}$ $\forall \mathfrak{p} \in \mathrm{Spec}R$ implies $Ann_R(I) = 0$. If I belongs to the set of zero-divisors then $I \subseteq \mathfrak{p} = Ann(x)$ for some x in R as it is Noetherian. This would contradict $Ann_R(I) = 0$.
To complete the proof, we must show that P_S is R_S-free. For notational simplicity we shall denote P_S by P, R_S by R and the *Jacobson ideal* of R by $j(R)$. We can reduce to the case $R/j(R)$: If P is R-free then $P \otimes_R R/j(R)$ is $R/j(R)$-free; conversely, if $P/j(R)P$ is $R/j(R)$-free, then let $0 \to K \to R^t \to P \to 0$ be tensored with $R/j(R)$. Flatness of P ensures the exactness of the resulting sequence (use Snake's lemma). Thus, $K \otimes_R R/j(R) = 0$ and by Nakayama, $K = 0$, $P \cong R^t$. In the reduced case, $R/j(R) = \bigoplus_{i=1}^n F_i$ and $P = \bigoplus_{i=1}^n P_i$ where P_i's are f.g. projective over F_i's (and hence free) of the same rank. Thus P is free and this completes the proof. ☐

4.2 R-sequences and grade

Let $a_1, a_2, \ldots, a_n$ be elements of R s.t. $(a_1, a_2, \ldots, a_n) \neq R$. The sequence $a_1, a_2, \ldots, a_n$ is called an **R-sequence** if $a_1 \notin \mathcal{Z}(R)$, $a_2 \notin \mathcal{Z}(R/(a_1)), \ldots,$ $a_n \notin \mathcal{Z}(R/(a_1, a_2, \ldots, a_{n-1}))$ or equivalently if $a_i \notin \cup\{\mathfrak{p} \in Ass(a_1, a_2, \ldots, a_{i-1})\}$, $i = 1, 2, \ldots, n$. Note that $0 <$ht $(a_1) < \cdots <$ht $(a_1, a_2, \ldots, a_n)$ as if ht $(a_1, a_2, \ldots, a_{i-1}) =$ ht $(a_1, a_2, \ldots, a_i)$, then any minimal prime of $(a_1, a_2, \ldots, a_i)$ of ht $(a_1, a_2, \ldots, a_{i-1})$ is also minimal over $(a_1, a_2, \ldots, a_i)$; hence $a_{i+1} \in \cup\{\mathfrak{p} \in Ass(a_1, a_2, \ldots, a_{i-1})\}$, a contradiction. Thus ht $(a_1, a_2, \ldots, a_n) \geqslant n$. Conversely, if $(a_1, a_2, \ldots, a_n)$ is a prime ideal of ht n in a local ring R, then by 2.1, $a_1, a_2, \ldots, a_n$ is an R-sequence.
Any R-sequence in I can be extended to an R-sequence which is maximal w.r.t. being contained in I. We shall show that any two such maximal R-sequences in I have the same length and is called the **grade** of I, denoted $G_R(I)$. We shall write $G(I)$ from now onwards when the ring is unambiguous. Note that :

$$G(I) \leqslant \text{ht } I \leqslant \mu(I)$$

Also, if $a_1, a_2, \ldots, a_n$ is an R-sequence in I, then this extends to an R_S-sequence if $(a_1, a_2, \ldots, a_n)R_S \neq R_S$, i.e., $G_R(I) \leqslant G_{R_S}(I_S)$ if $I_S \neq R_S$. Further, if $(a_1, a_2, \ldots, a_n)$ is a maximal R-sequence in I, then $I \subset \cup\{$primes in $Ass(a_1, a_2, \ldots, a_n)\}$; the union is finite as R is Noetherian. So $I \subset \mathfrak{p} \subset \mathcal{Q}$ where $\mathcal{Q}$

is an associated prime and $\mathfrak{p}$ is a minimal one in it containing I. Hence $G(I) = G(\mathfrak{p}) = G(\mathcal{Q})$ and $G(I) = \inf\{G(\mathfrak{p}) | \mathfrak{p} \in V(I)\}$.

Theorem 4.2. *$G(I) = \mu(I)$ iff I is generated by an R-sequence. Moreover, if I is generated by an R-sequence and $I \subset j(R)$, then any minimal generating set for I is an R-sequence.*

To prove this we require an easy lemma :

Lemma 4.3. *Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ be prime ideals in R, let I be an ideal in R, and x an element of R s.t. $(x, I) \not\subset \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_n$. Then there exists $i \in I$ s.t. $x + i \notin \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_n$.*

Proof : We may assume that no two of the $\mathfrak{p}$'s are comparable, for any $\mathfrak{p}_k$ contained in another can simply be deleted without changing the problem. Suppose that x lies in $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ but not in any of $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_n$ (if $r = 0$, $i = 0$ will do, and if $r = n$ the following proof applies with $y = 1$). We have $I \not\subset \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_r$. Thus there is $i_0 \in I$ but not in any of $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Next choose y in $\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n$ but not in $\mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_r$. We can do so, for otherwise $\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n \subset \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_r$, whence $\mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_n \subset \mathfrak{p}_j$ for some $j (1 \leqq j \leqq r)$, and $\mathfrak{p}_k \subset \mathfrak{p}_j$ $(r + 1 \leqq k \leqq n)$ for some k, a contradiction. The element $i = y i_0$ then satisfies our requirement. □

Proof of theorem : Let $G(I) = \mu(I) = k$ and set $I = (x_1, x_2, \ldots, x_k)$. We will find elements $u_1 = x_1$+linear combination of $x_2, \ldots, x_k$, $u_2 = x_2$+linear combination of $x_3, \ldots, x_k$,... constituting a sort of change of basis, s.t. the u_i's form an R-sequence, by repeated application of 4.3.
We may assume $k > 0$. Since $I \not\subset \mathcal{Z}(R)$ apply 4.3with $x = x_1$, $I' = (x_2, \ldots, x_k)$ and $\mathcal{Z}(R) = \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_n$. With i from 4.3 set $u_1 = x + i$. If $k = 1$ we are done. So suppose that $I \not\subset \mathcal{Z}(R/(u_1))$. Then it follows that $(x_2, \ldots, x_k) \not\subset \mathcal{Z}(R/(u_1))$. Suppose not, then any $i \in I$ can be written as $i = \sum_{s=i}^{k} a_s x_s$ $(a_s \in R)$ and this can be rewritten as $i = a_1 u_1 + b_2 x_2 + \cdots + b_k x_k$ $(b_s \in R)$. Since $a_1 u_1$ annihilates $R/(u_1)$ and $b_2 x_2 + \cdots + b_k x_k$ is a zero-divisor on $R/(u_1)$, we get $I \subset \mathcal{Z}(R/(u_1))$, a contradiction. Now apply 4.3 with $x = x_2$, $I = (x_3, \ldots, x_k)$, and $\mathcal{Z}(R/(u_1)) = \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_n$. If i is the resulting element then we put $u_2 = x_2 + i$. Continue in this way to terminate at the kth stage whence $u_1, u_2, \ldots, u_k$ generate I. □

4.3 The main theorem

What we shall prove is part of a bigger theorem that is true in a more general setting of Noetherian rings (not necessarily UFD) and it further states that :
If I is a regular ideal s.t. $d(I) = 1$, then $I = I_0 I^*$, where I_0 is an invertible ideal and I^* is a proper ht 2, grade 2, grade-unmixed ideal; and the converse holds if R is Cohen-Macaulay and all maximal ideals have ht 3.
Since our primary concern will be "when $d(I) = 1$" and $R = k[X_1, X_2, X_3]$ will be UFD anyway, we shall prove for R Noetherian UFD.

Theorem 4.4. *Suppose $d(I) < \infty$. If $sup\{\mu(I_{\mathfrak{p}}) | \mathfrak{p} \in V(I)\} = 2$, then $d(I) = 1$.*

Proof : Let us note that the hypothesis implies $d(I) > 0$. For, if not, then I is locally free of rank 1, a contradiction. Let G be the *gcd* of elements of I. Then $I = (g)I^*$ where I^* is a non-zero ideal of *gcd* 1. Moreover, $I^* \neq R$ as then I would be f.g. regular and locally principal (hence $d(I) = 0$). Choose $a \neq 0 \in I^*$ and write $a = a_1 a_2 \ldots a_t$ into irreducible factors. Then $I^* \not\subset (a_i)$ as *gcd* $I^* = 1$, whence $I \not\subset \bigcup_{i=1}^{t} (a_i)$ as $(a_i) \in \operatorname{Spec} R$. Hence choose $b \in I^*$ s.t. b and a have no common (irreducible) factors, from which it is clear that a, b is a R-sequence. Thus $G(I^*) \geqslant 2$.

$\mu(I) \leqslant 2$ locally implies $\mu(I^*) \leqslant 2$ locally and for $\mathfrak{p} \in V(I^*)$, $2 \leqslant G(I^*) \leqslant G(I^*_{\mathfrak{p}}) \leqslant \mu(I^*_{\mathfrak{p}}) \leqslant 2$. So by 4.2 $I^*_{\mathfrak{p}}$ is generated by a $R_{\mathfrak{p}}$-sequence of length 2 and hence by Koszul resolution (cf 5.1), $d(I^*_{\mathfrak{p}}) \leqslant 1$ implying $d(I^*) = 1$ and so is $d(I)$. $\square$

REMARKS : (a) For $R = k[X_1, X_2, X_3]$ and I, the defining ideal of a non-singular unmixed variety of dimension 1 in $\mathbf{A}^3_k$, satisfies the hypothesis and $d(I)$ is finite by **??**; hence $d(I) = 1$.
(b) $I^{-1} \cong \mathrm{Hom}_R(I, R)$, if $I \neq R$ is a regular ideal of R. To see this, take $\xi \in I^{-1}$, then multiplication by ξ gives an element of $\mathrm{Hom}_R(I, R)$. Conversely, given $h \in \mathrm{Hom}_R(I, R)$, fix an element $a \in I$ which is regular. then putting $\xi = \frac{h(a)}{a}$, we have : $\xi x = h(x)$.

5 $\mathbf{Ext}^1_R(I, R) \cong \Omega_k(R/I)$

We have already seen in §3 that for a ht 2 unmixed ideal I of $R = k[X_1, X_2, X_3]$ which is locally a c.i., $\mu(I) = 2$ iff $\mu(\mathrm{Ext}^1_R(I, R)) = 1$. We'll next show that $\mathrm{Ext}^1_R(I, R)$ depends only on R/I for any non-singular unmixed curve in $\mathbb{A}^3_k$. This follows once we establish the following isomorphism :

$$\mathrm{Ext}^1_R(I, R) \cong \mathrm{Hom}_{R/I}(\textstyle\bigwedge^2(I/I^2), R/I) \cong \Omega_k(R/I)$$

Here $\Omega_k(R/I)$ is the module of k-differentials of R/I. In §5.1-5.3, I will be assumed to be generated by a R-sequence of length 2, i.e., we are working locally. We patch up these local isomorphisms to get a global one and finally discuss the isomorphism relating $\mathrm{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I)$ and $\Omega_k(R/I)$.

5.1 The Koszul resolution

Let $I = (a_1, a_2)$ be s.t. a_1, a_2 is a R-sequence. Denote $\mathcal{K}(a_1, a_2)$ by the s.e.s : $0 \to R \overset{\varphi}{\to} R^2 \overset{\psi}{\to} I \to 0$ s.t. $\varphi(e) = (a_2, -a_1)$ and $\psi(e_i) = a_i, i = 1, 2$. Note that exactness follows from $\psi \circ \varphi = 0$ and $ker\ \psi$ being freely generated by $(a_2, -a_1)$.
Suppose that a'_1, a'_2 be another R-sequence that generates I. Let $a_i = r_{i1}a'_1 + r_{i2}a'_2, i = 1, 2$ and let $r = det(r_{ij})$. Then the following diagram commutes :

$$\begin{array}{llllllllll}
\mathcal{K}(a_1, a_2) : & 0 & \longrightarrow & R & \longrightarrow & R^2 & \longrightarrow & I & \longrightarrow & 0 \\
 & & & \downarrow \alpha & & \downarrow \delta & & \| & & \\
\mathcal{K}(a'_1, a'_2) : & 0 & \longrightarrow & R & \longrightarrow & R^2 & \longrightarrow & I & \longrightarrow & 0
\end{array}$$

where $\delta(e_i) = r_{i1}e_1 + r_{i2}e_2$ and $\alpha(e) = r$. One can get α by computing for commutativity. Thus in $\mathrm{Ext}^1_R(I, R)$, $r.[\mathcal{K}(a_1, a_2)] = [\mathcal{K}(a'_1, a'_2)]$.

5.2 $\mathbf{Ext}^1_R(I, R) \cong R/I$

Apply $\mathrm{Hom}_R(\_, R)$ to $\mathcal{K}[(a_1, a_2)]$ to get the following commutative diagram :

$$\begin{array}{ccccccc}
Hom_R(R^2, R) & \xrightarrow{\nu} & Hom_R(R, R) & \xrightarrow{\eta} & Ext^1_R(I, R) & \longrightarrow & 0 \\
\Big\| & & \Big\downarrow \tau & & \Big\downarrow \rho & & \\
Hom_R(R^2, R) & \xrightarrow{\tau \circ \nu} & R & \longrightarrow & R/I & \longrightarrow & 0
\end{array}$$

The top row is exact and $\eta(id) = [\mathcal{K}(a_1, a_2)]$. Also, τ is just the evaluation map at id and $R \to R/I$ is the canonical map. Define $\rho : [\mathcal{K}(a_1, a_2)] \mapsto id$ in R/I. For $\alpha \in \mathrm{Hom}_R(R^2, R)$, $\tau \circ \nu(\alpha) = \nu(\alpha)(e)$ $= \alpha \circ \phi(e) = \alpha(a_2, -a_1) = r_1 a_2 - r_2 a_1 \in I$. Conversely, let $i = r_1 a_2 - r_2 a_1 \in I$. Defining $\alpha : R^2 \to R$ by $\alpha(e_i) = r_i, i = 1, 2$ gives $\tau \circ \nu(\alpha) = i$. Thus the bottom row is exact and ρ is an isomorphism as τ is!
We note here that if a different R-sequence was used and the resulting isomorphism was ρ', then we would have $det(r_{ij})\rho' = \rho$.

5.3 $\mathbf{R/I} \cong \mathbf{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I)$

Lemma 5.1. *If an ideal J of R is generated by a R-sequence $a_1, a_2, \ldots, a_t$, then J/J^2 is R/J-free on $a_1^*, a_2^*, \ldots, a_t^*$, where a_i^*'s denote the images of a_i's in J/J^2.*

Proof : It suffices to show that $\sum_{i=1}^t a_i^* r_i = 0$ in J/J^2 (i.e., $\sum_{i=1}^t a_i r_i \in J^2$) then $r_i = 0$ in R/J (i.e., $r_i \in J$). If $t = 1$ then $r_1 a_1 \in J^2$ means $r_1 \in J$ as $a_1 \notin \mathcal{Z}(R)$. So we assume $t > 1$ and induct on t. Since $\sum_{i=1}^t a_i r_i \in J^2$, write it $\sum_{i=1}^t a_i r_i = \sum_{i=1}^t a_i c_i$, $c \in J$. Then setting $r'_i = r_i - c_i$ we get $r'_i \equiv r_i \bmod J$ and $\sum_{i=1}^t a_i r'_i = 0$. Going modulo $(a_1, \ldots, a_{t-1})$, $r'_t a_t = 0$ in $R/(a_1, a_2, \ldots, a_{t-1})$. But $a_t \notin \mathcal{Z}(R/(a_1, a_2, \ldots, a_{t-1}))$ and hence $r'_t \in (a_1, \ldots, a_{t-1})$. So, $\sum_{i=1}^{t-1} a_i r'_i \in J^2$. By previous remarks can get r''_i s.t. $\sum_{i=1}^{t-1} a_i r''_i = 0$ and $r''_i \equiv r'_i \equiv r_i \bmod J$. Induction hypothesis applied to $I = (a_1, a_2, \ldots, a_{t-1})$ gives $r''_i \in I \subseteq J$, and we're done. □

Consequently, for our ideal I, generated by a R-sequence a_1, a_2, $\bigwedge^2(I/I^2)$ is R/I-free of rank 1 and there is an isomorphism as stated. More precisely, since $\bigwedge^2(I/I^2)$ is R/I-free on $a_1^* \wedge a_2^*$, $\sigma(a_1, a_2) : \mathrm{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I) \to R/I; h \mapsto h(a_1^* \wedge a_2^*)$ is the isomorphism we're looking for. If we choose another R-sequence a'_1, a'_2 for I, and let σ' be the corresponding isomorphism, then $a_1^* \wedge a_2^* = det(r_{ij}^*)(a_1^{'*} \wedge a_2^{'*})$ and hence $\sigma = det(r_{ij}^*)\sigma'$.
This partly gives the isomorphism stated in §5 :

$$\mathrm{Ext}^1_R(I, R) \xrightarrow{\rho} R/I \xrightarrow{\sigma^{-1}} \mathrm{Hom}_{R/I}(\textstyle\bigwedge^2(I/I^2), R/I)$$

Now $\sigma^{-1} \circ \rho = \sigma'^{-1} \circ \rho'$ as the isomorphism above can be regarded as that of R/I-modules or R-modules.

5.4 The global isomorphism

The following lemma shows that the property of being generated locally (at a prime $\mathfrak{p}$) by a regular sequence can be spread out to a neighborhood of $\mathfrak{p}$.

Lemma 5.2. *Let $I \neq R$ be an ideal of a Noetherian ring R and let $\mathfrak{p} \in V(I)$. If $I_\mathfrak{p}$ is generated by a regular sequence of length t, then there exists $s \notin \mathfrak{p}$ s.t. I_s is generated by a regular sequence of length t.*

Proof : We know that there exist $a_i, i = 1, 2, \ldots, t \in I$ s.t. $a_1/1, a_2/1, \ldots, a_t/1$ is a $R_{\mathfrak{p}}$-sequence generating $I_{\mathfrak{p}}$. Since I is f.g., $\exists s_0 \notin \mathfrak{p}$ s.t. $s_0 I \subset (a_1, \ldots, a_t)$. Moreover $\{\mathfrak{q} \in Ass(a_1, \ldots, a_{i-1}) | \mathfrak{q} \not\subset \mathfrak{p}\}$ is non-empty and finite. Since none of the $\mathfrak{q}$'s lie in $\mathfrak{p}$, $\exists s_i \notin \mathfrak{p}$ s.t. $s_i \in \cap\{\mathfrak{q} \in Ass(a_1, \ldots, a_{i-1}) | \mathfrak{q} \not\subset \mathfrak{p}\}$, $i = 1, 2, \ldots, t$. Put $s = s_0 s_1 \cdots s_t$. Then $a_1/1, \ldots, a_t/1$ generate I_s. Notice that $a_1/1 \notin \mathcal{Z}(R_s)$ as it is not a zero-divisor in $I_{\mathfrak{p}}$ and we have inverted s_1 (which lies in all associated primes of (0) which do not lie in $\mathfrak{p}$). Similarly, $a_i/1 \notin \mathcal{Z}(R_s/(a_1/1, \ldots, a_{i-1}/1)), i = 1, 2, \ldots, t$. □

Our next proposition enables us to patch together a collection of neighborhood homomorphisms to a global one.

Proposition 5.3. *Let $s_1, \ldots, s_n$ be elements of a ring R s.t. $(s_1, \ldots, s_n) = R$. Let M, N be R-modules equipped with R_{s_i}-module homomorphisms $\phi_i : M_{s_i} \to N_{s_i}, i = 1, 2, \ldots, n$. For $i \neq j$, let ϕ_{ij} denote the R_{ij}-module homomorphism which makes the following commute:*

$$\begin{array}{ccc} M_{s_i s_j} & \xrightarrow{\phi_{ij}} & N_{s_i s_j} \\ \uparrow & & \uparrow \\ M_{s_i} & \xrightarrow{\phi_i} & N_{s_i} \end{array}$$

If $\phi_{ij} = \phi_{ji}$ for $i \neq j$ then there exists a R- module homomorphism $\Phi : M \to N$, s.t. $\Phi_i = \phi_i$ $\forall$ $i = 1, 2, \ldots, n$.

Proof : The main idea behind defining Φ is the following :
Let N be a R-module and suppose $s_1, \ldots, s_n \in R$ s.t. $(s_1, \ldots, s_n) = R$. We shall denote N_{s_i} by N_i for convenience. Given $a_i \in N_i$ $\forall i = 1, \ldots, n$ s.t. a_i and a_j are same in N_{ij} for $i \neq j$, we get an unique element $a \in N$ s.t. the canonical image of a in N_i is $a_1, i = 1, \ldots, n$.
To see this, assume $a_i = n_i/s_i^k$, (can assume the exponent of s_i occuring in the representation of a_i to be k for all the i's by taking the maximum if necessary). Since $a_i = a_j$ in N_{ij}, $n_i s_j^k (s_i s_j)^l = n_j s_i^k (s_i s_j)^l$; here again can take l to be same for all $i \neq j$ and further take $k = l$. Then we have :

$$n_i s_i^k s_j^{2k} = n_j s_j^k s_i^{2k} \ \forall \ i \neq j \ ... \ (\dagger)$$

Since $s_1, \ldots, s_n$ generate R, so does $s_1^{2k}, \ldots, s_n^{2k}$. Writing $1 = \sum_{i=1}^n f_i s_i^{2k}$ and putting $n_0 = \sum_{i=1}^n f_i s_i^k n_i$, an easy computation (using (†)) shows that $s_i^{2k} n_0 = s_i^k n_i$, whence $n_0/1 = a_i$. Uniqueness of n_0 is clear because if n_0', $n_0 \in N$ satisfy the requirements, then $s_i^k(n_0 - n_0') = 0$ $\forall$ $i = 1, \ldots, n$ and $(s_1^k, \ldots, s_n^k) = R$.
Now for any $m' \in M$, let $a_i = \phi_i(m'/1)$ and get a unique $n' \in N$ (by the above discussion) and define Φ by mapping m' to n'. This defines a well-defined map $\Phi : M \to N$, which is a homomorphism. □

REMARKS : (a) Each s_i defines an open set $U_i = \{\mathfrak{p} \in \text{Spec}R \mid s_i \notin \mathfrak{p}\}$. The condition translates to $\text{Spec}R = \cup_{i=1}^n U_i$.
(b) If each ϕ_i is an isomorphism, then so is Φ : Let $m \in ker\ \Phi$. Then $\Phi_i(m/1) = 0$ (i.e. $s_i^r m_i = 0$) $\forall$ $i = 1, \ldots, n$ and hence $m = 0$. Φ is onto because of the construction. Thus it is an isomorphism.
(c) If $I \neq R$ is s.t. $I \subseteq AnnN \cap AnnM$ (or if M and N can be regarded as R/I-modules) then for applying the proposition to R/I it suffices to assume that $(s_1, s_2, \ldots, s_n, I) = R$.

Theorem 5.4. *Let $I \neq R$ be an ideal R, a Noetherian ring, s.t. I is locally generated by a regular sequence of length 2 at every prime containing I. Then $Ext_R^1(I, R) \cong Hom_{R/I}(\bigwedge^2(I/I^2), R/I)$.*

Proof : For each $\mathfrak{p} \in V(I)$, $\exists\ s = s_{\mathfrak{p}} \notin \mathfrak{p}$ s.t. I_s is generated by a regular sequence of length 2, by 5.2. Then no prime contains the ideal generated by $s_{\mathfrak{p}}$'s and I. Since R is Noetherian, the ideal generated by $s_{\mathfrak{p}}$'s can be generated by $s_1, \ldots, s_n$ s.t. $(s_1, \ldots, s_n, I) = R$.
We drop the s's from the notation for simplicity. Let a_i, b_i be a regular sequence which generate I_i and let a_{ij}, b_{ij} denote the canonical images of a_i, b_i in R_{ij}. By §5.3, $\exists\ \Gamma_i$ and Γ_{ij} defined w.r.t. a_i, b_i and a_{ij}, b_{ij} s.t. the following diagram commutes :

$$\begin{array}{ccc} \mathrm{Ext}^1_{R_{ij}}(I_{ij}, R_{ij}) & \xrightarrow{\Gamma_{ij}} & \mathrm{Hom}_{R_{ij}/I_{ij}}(\bigwedge^2(I_{ij}/I_{ij}^2), R_{ij}/I_{ij}) \\ \uparrow & & \uparrow \\ \mathrm{Ext}^1_{R_i}(I_i, R_i) & \xrightarrow{\Gamma_i} & \mathrm{Hom}_{R_i/I_i}(\bigwedge^2(I_i/I_i^2), R_i/I_i) \end{array}$$

Moreover $\Gamma_{ij} = \Gamma_{ji}$ since the Γ_i's were independent of the regular sequences chosen. Note that $\mathrm{Hom}_{R_i/I_i}(\bigwedge^2(I_i/I_i^2), R_i/I_i) \cong \mathrm{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I)_i$ as $\bigwedge^2(I/I^2)$ is f.p. and $\mathrm{Ext}^1_{R_{ij}}(I_{ij}, R_{ij}) \cong \mathrm{Ext}^1_{R_i}(I_i, R_i)_j = (\mathrm{Ext}^1_R(I, R)_i)_j \cong \mathrm{Ext}^1_R(I, R)_{ij}$ as I is f.p. Making these necessary identifications in the diagram above gives the required diagram as per 5.3 and thus we have the necessary global isomorphism. □

5.5 $\mathbf{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I) \cong \Omega_k(R/I)$

We shall begin by listing a few elementary properties of $\otimes$ and $\wedge$:
(a) Let A, B be ideals of R. There is a surjective map $h : A \otimes_R B \to AB$, taking $a \otimes b$ to ab. If B is flat, then $0 \to A \to R$ on tensored with B gives $0 \to A \otimes_R B \to B$; so h is an isomorphism.
(b) Let A, B be R-modules. Note that $\wedge^n(A \oplus B) \cong \bigoplus_{i=0}^n [\wedge^i A \otimes_R \wedge^{n-i} B]$. Moreover, if A is free of rank t then $\wedge^t A \cong R$ and $\wedge^{t+i} A = 0$ for $i \geqslant 1$. Also, since localization commutes with tensoring and quotients, $\wedge^t_{R_S} A_S \cong (\wedge^t A)_S$ for any mult. closed subset S of R. Thus if A is locally free of constant rank t, then $\wedge^t A$ is locally free of constant rank 1.
(c) Suppose A is a f.g. R-projective of constant rank t and we have a B s.t. $A \oplus B \cong R^n$ (B is f.g. proj. of const. rk $n - t$). Now by (b) above, $R \cong \wedge^t A \otimes_R \wedge^{n-t} B$ and $\wedge^t A$, $\wedge^{n-t} B$ are locally free of rank 1. Hence by 4.1, they are isomorphic to invertible ideals P, Q resp. Thus $PQ \cong P \otimes_R Q \cong R$; the first isomorphism follows from (a), the second from (b) and the discussion above. Hence $PQ = rR$ for some regular element $r \in R$ and $Q = rP^{-1} \cong P^{-1}$ and $P^{-1} \cong \mathrm{Hom}_R(P, R)$ by remarks following 4.4. Thus : $\wedge^{n-t} B \cong \mathrm{Hom}_R(\wedge^t A, R)$.
Combining (c) above with 5.4 and the isomorphism of 5.3, we have :

Theorem 5.5. *Suppose $I \neq R$ be an ideal in a Noetherian ring R which is locally generated by a regular sequence of length 2 (at all primes containing I). Then :*
(i) I/I^2 is R/I-projective of constant rank 2
(ii) $Ext^1_R(I, R) \cong Hom_{R/I}(\bigwedge^2(I/I^2), R/I)$ and
(iii) If B is s.t. $(I/I^2) \oplus B \cong (R/I)^n$, then $Hom_{R/I}(\bigwedge^2(I/I^2), R/I) \cong \wedge^{n-2} B$.

We shall observe in the what follows after 6.5 that if $R = k[X_1, X_2, \ldots, X_n]$, k a perfect field, I is a ht t unmixed ideal s.t. R/I is regular, then $(I/I^2) \oplus \Omega_k(R/I) \cong (R/I)^n$. Then for $R = k[X_1, X_2, X_3]$, k perfect, and I, a ht 2 unmixed ideal of R, $\mathrm{Ext}^1_R(I, R) \cong \Omega_k(R/I)$ using 5.5.

6 The module of differentials

The main object of study in this section will be the module of differentials.

6.1 Definitions and Properties

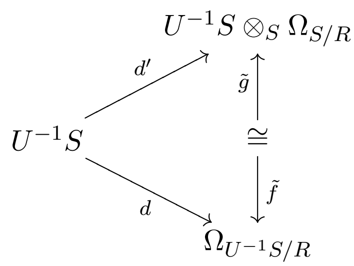
If S is a ring, M is an S-module, then a map (of abelian groups) $d : S \to M$ is a **derivation** if it satisfies the **Leibnitz rule** i.e.,

$$d(fg) = fd(g) + gd(f) \ \forall \ f, g \in S$$

If S is a R-algebra, then we say d is R-linear if it is a map of R-modules. Notice that $d(1) = 0$ and hence d is R-linear iff $da = 0 \ \forall a \in R$.
If S is a R-algebra, then **the module of Kähler differentials** of S over R, written $\Omega_{S/R}$ or $\Omega_R(S)$, is the S-module generated by the formal symbols $\{df | f \in S\}$ subject to the relations $d(bb') = bd(b') + b'd(b)$ and $d(ab + a'b') = ad(b) + a'd(b') \ \forall a, a' \in R$ and $b, b' \in S$. This makes $d : S \to \Omega_{S/R}$, sending d to df, a R-linear derivation. Equivalently, this can be thought of as the universal object in the category of R-linear derivations and S-modules (i.e.,if $\delta : S \to M$, a derivation s.t. δ is R-linear, then it factors uniquely through $\Omega_{S/R}$. Thus this module is unique up to isomorphism.

1. If S is a R-algebra generated by f_i's, then $\Omega_{S/R}$ is generated as an S-module generated by df_i's. In particular, $\Omega_{S/R}$ is f.g. as an S-module whenever S is f.g. as a R-algebra. If $S = R[x_1, x_2, \ldots, x_r]$, x_i's indeterminates, then $\Omega_{S/R} = \oplus_{i=1}^{r} S dx_i$, the free module on the dx_i's as $\Omega_{S/R}$ is generated by the dx_i's and there is an onto homomorphism taking S^r to $\Omega_{S/R}$ by mapping e_i's to dx_i's. On the flip side, $\frac{\partial}{\partial x_i}$ is a R-linear derivation from S to S inducing an S-module map $\partial_i : \Omega_{S/R} \to S$ carrying dx_i to 1 and rest to 0. Putting these together we get the required isomorphism.

2. **Localization commutes with** Ω : Let S be an R-algebra and U be a mult. closed subset of S. Then $\Omega_{U^{-1}S/R} \cong \Omega_{S/R} \otimes U^{-1}S$. To see this, define $d' : U^{-1}S \to U^{-1}S \otimes_S \Omega_{S/R}$ by sending $1/s$ to $s^{-2}ds$, $b/1$ to db and extending by Leibniz rule. We want a commutative diagram :



   The composition $S \to U^{-1}S \to \Omega_{U^{-1}S/R}$ is a derivation and thus we have a map f from $\Omega_{S/R}$ to $\Omega_{U^{-1}S/R}$. To define the downward map, take $\tilde{f} = f \otimes 1$ as the map. More specifically, $\tilde{f} : dc \otimes b/s \mapsto b/s \ d(c/1)$. To define the upward map $\tilde{g}$ we send $d(b/s)$ to $(1/s^2)(sdb - bds)$ and check that it is well-defined. If $b/s = 0$ then some $s' \in U$ kills b (so that $b/t = 0$ for all $t \in S$) and thus s'^2 kills db (as $d(s'^2 b) = 0$), whence $d(b/t) = 0$.

3. **Relative Cotangent Sequence** : *If $R \to S \to T$ are maps of rings, then there is a right-exact sequence of T-modules* :

$$T \otimes_S \Omega_{S/R} \xrightarrow{D\pi} \Omega_{T/R} \xrightarrow{\psi} \Omega_{T/S} \to 0.$$

Here $D\pi(c \otimes db) = cdb$ and $\psi(dc) = dc$. This is so as the generators for $\Omega_{T/S}$ is the same as that of $\Omega_{T/R}$ but with the extra relations that $db = 0\ \forall b \in S$. But these are precisely the images of the generators $1 \otimes db$ of $T \otimes_S \Omega_{S/R}$.

4. **Conormal Sequence** : *If $\pi : S \to T$ is a surjective homomorphism of R-algebras, with kernel I, then there is an exact sequence of T-modules*

$$I/I^2 \xrightarrow{\phi} T \otimes_S \Omega_{S/R} \xrightarrow{D\pi} \Omega_{T/R} \to 0$$

where $D\pi$ maps $c \otimes db$ to cdb and ϕ takes the class of f to $1 \otimes df$.
Observe that $\Omega_{T/S} = 0$ by S-linearity and the fact that any $t \in T$ has a pre-image in S. Consider the restriction $d : I \to \Omega_{S/R}$ of $d : S \to \Omega_{S/R}$. If $b \in S, c \in I$ then by Leibnitz, $d(bc) = bdc + cdb$ shows that d induces an S-linear map $I \to (\Omega_{S/R})/(I\Omega_{S/R}) = T \otimes_S \Omega_{S/R}$. If $b \in I$ in the above, then I^2 goes to 0 in $T \otimes_S \Omega_{S/R}$. This provides ϕ.

We shall describe $T \otimes_S \Omega_{S/R}$ by generators and relations. Since tensoring is right-exact, $- \otimes_S T$ on $0 \to$Module of R-linearity, Leibnitz relations$\to$Free on $\{ds | s \in S\} \to \Omega_{S/R}$ gives that $T \otimes_S \Omega_{S/R}$ is generated as a T-module by the elements db for $b \in S$ modulo the relations of R-linearity and Leibnitz rule. In $\Omega_{T/R}$, the same generators generate but df for $f \in I$ are 0 as I is the kernel. So, the cokernel of $d : I/I^2 \to T \otimes_S \Omega_{S/R}$ is $D\pi$ and the exactness is verified.

5. *If $T = \otimes_R S_i$ is the coproduct of some R-algebras S_i, then*

$$\Omega_{T/R} \cong \oplus_i (T \otimes_{S_i} \Omega_{S_i/R}) = \oplus_i ((\otimes_{R,j \neq i} S_j) \otimes_R \Omega_{S_1/R}$$

For the equality, notice that

$$T \otimes_{S_i} \Omega_{S_i/R} = (\otimes_{R,j \neq i} S_j) \otimes_R S_i \otimes_{S_i} \Omega_{S_i/R} = (\otimes_{R,j \neq i} S_j) \otimes_R \Omega_{S_i/R}$$

Let d_i denote the universal derivation of S_i and Ω denote $\oplus_i((\otimes_{R,j \neq i} S_j) \otimes_R \Omega_{S_1/R}$. Any element of T involves finite sums of terms $\otimes b_i$ and in each term only finitely many b_i's different from 1 are involved. Thus only finitely many of the maps

$$1 \otimes d_i : T = (\otimes_{R,j \neq i} S_j) \otimes_R S_i) \to (\otimes_{R,j \neq i} S_j) \otimes_R \Omega_{S_i/R}$$

are non-zero on any element. So the map $e : T \to \Omega$ defined by the sum $\sum_i 1 \otimes d_i$ is a (well-defined) derivation as each map is! Hence there is an induced T-module homomorphism $\alpha : \Omega_{T/R} \to \Omega$.

We shall construct the inverse of α. The composite map $S_i \to T \to \Omega_{T/R}$ is naturally a R-linear derivation and thus induces an S_i-linear map $\Omega_{S_i/R} \to \Omega_{T/R}$ sending $d_i b_i$ to $d(\cdots \otimes 1 \otimes 1 \otimes b_i \otimes 1 \otimes 1 \otimes \cdots)$ with the b_i occuring in the ith place. This extends to a T-linear map (as $\Omega_{T/R}$ is a T-module) $\beta_i : T \otimes_{s_i} \Omega_{S_i/R} \to \Omega_{T/R}$ with $1 \otimes d_i b_i$ being sent to $d(\cdots \otimes 1 \otimes 1 \otimes b_i \otimes 1 \otimes 1 \otimes \cdots)$. Then β_i together give a map $\beta : \Omega \to \Omega_{T/R}$. Now $\alpha \circ \beta(\cdots, 1 \otimes d_i b_i, \cdots) = \alpha(\cdots, d(1 \otimes b_i), \cdots)$ $= \sum_i (1 \otimes d_i)(\sum_{finite}(1 \otimes b_i)) = (\cdots, 1 \otimes d_i b_i, \cdots)$. Similarly $\beta \circ \alpha = id$. Hence we have the stated isomorphism.

6. *If $T = S[x_1, \ldots, x_r]$ is a polynomial ring over an R-algebra S, then*

$$\Omega_{T/R} \cong (T \otimes_S \Omega_{S/R}) \oplus (\oplus_i T dx_i)$$

This is clear once we observe that $T = S \otimes_R R[x_1, \ldots, x_r]$, $\Omega_{R[x_1,\ldots,x_r]/R} = \oplus_i R dx_i$ and use the previous result.

7. *Let $R \to S \subset T$ be maps of rings. If S and T are fields and T is finite separable extension of S, then $\Omega_{T/R} = T \otimes_S \Omega_{S/R}$.*
   To see this, choose a primitive element $\alpha \in T$. If f is the minimal polynomial of α we have $T = S[x]/f$. The conormal sequence for $R \to S[x] \to T$ is

$$(f)/(f^2) \xrightarrow{d} T \otimes_{S[x]} \Omega_{S[x]/R} \to \Omega_{T/R} \to 0,.$$

   where the left-hand map sends $f + (f^2)$ to $1 \otimes df$. Applying the previous result we get

$$\Omega_{S[x]/R} \cong S[x] \otimes_S \Omega_{S/R} \oplus S[x]dx$$

   and so

$$T \otimes_{S[x]} \Omega_{S[x]/R} \cong T \otimes_S \Omega_{S/R} \oplus T dx.$$

   The component of $1 \otimes df$ in Tdx under this map is $f'(\alpha)dx$. Since T is separable over S, $f'(\alpha) \neq 0$ and $f'(\alpha)dx$ generates Tdx. Thus $\Omega_{T/R} \cong$ *coker* d, which is $T \otimes_S \Omega_{S/R}$ by the deductions above.

8. Let $k \subset K$ be fields with K finitely generated over k. For k perfect, any extension is separably generated. Also, if K is separably algebraic over k, $\Omega_{K/k} = 0$ and this can be seen by taking any α and f to be the minimal polynomial of α over k and noting that $f'(\alpha)d\alpha = 0$ whereas $f'(\alpha) \neq 0$. Then assuming k perfect, we have $k \subset L \subset K$ to be a tower of fields s.t. $L = k[x_1, x_2, \ldots, x_n]$ is purely transcendental over k with $n = tr.deg = tr.deg(K/k)$ and K is finite separable over L. By the above discussion, $\Omega_{K/k} = K \otimes_L \Omega_{L/k} \cong K \otimes_L \oplus_{i=1}^n L dx_i$. Thus $\mu(\Omega_{K/k}) = tr.deg(K/k)$.

6.2 Rank $\Omega_k(R/I)$

In this part we try to find conditions as to when ϕ of the conormal sequence is injective. When this is so, by the conormal sequence of $k \to R(= k[X_1, \ldots, X_n]) \to R/I$ we have the exact sequence :

$$0 \to I/I^2 \xrightarrow{\phi} (R/I)^n \xrightarrow{D\pi} \Omega_k(R/I) \to 0$$

Suppose that k is a field, A is a f.g. k-algebra which is also a domain s.t. $A_{(0)}$ is separably generated over k. Then rk $\Omega_k(A) = \mu(\Omega_k(A)_{(0)}) = \mu(\Omega_k(A_{(0)})) = tr.deg(A_{(0)}/k) = \dim A$; the first equality is by definition, the second by property 2 of 6.1, the third by property 7 of 6.1 and the last from dimension theory. In a more general setup,

Proposition 6.1. *Let k be a field and A be a reduced f.g. k-algebra such that $A_\mathfrak{p}$ is separably generated over k for every ht 0 prime $\mathfrak{p} \in SpecA$. Then $\mu((\Omega_k(A))_\mathfrak{p}) = dim\ A/\mathfrak{p}$.*

Proof : Since A is reduced, $\mathfrak{p}$ is of ht 0, $A_\mathfrak{p}$ is also reduced and $\mathfrak{p}A_\mathfrak{p} = 0$, thereby implying that $A_\mathfrak{p} = (A/\mathfrak{p})_{(0)}$. Further $\mu((\Omega_k(A))_\mathfrak{p}) = \mu(\Omega_k(A_\mathfrak{p})) = \mu(\Omega_k((A/\mathfrak{p})_{(0)}))$, which equals dim $A/\mathfrak{p}$ by the beginning statements. ☐

Lemma 6.2. *Let R be the polynomial ring in n variables over a field k and let I be a radical ideal of R s.t. $(R/I)_{\mathfrak{q}}$ is separably generated over k for every minimal prime $\mathfrak{q}$ of I. Then for any prime $\mathfrak{p} \supseteq I$, rk $K_{\mathfrak{p}} =$ ht $I_{\mathfrak{p}}$, where $K =$ Im ϕ.*

Proof : Since R/I is reduced, $(R/I)_{\mathcal{Q}}$ is a field for any minimal prime $\mathcal{Q}$ of I; and thus adding ranks $\mu(K_{\mathcal{Q}}) = n - \mu(\Omega_k(R/I)_{\mathcal{Q}}) = n-$ coht $\mathcal{Q} =$ ht $\mathcal{Q}$, the penultimate equality following from the previous proposition. So, rk $K_{\mathfrak{p}} = \inf\{\mu(K_{\mathcal{Q}}|\mathcal{Q}$ is a minimal prime of I and $\mathcal{Q} \subset \mathfrak{p}\} = \inf\{$ht $\mathcal{Q}|\mathcal{Q}$ is a minimal prime of I and $\mathcal{Q} \subset \mathfrak{p}\} =$ ht $I_{\mathfrak{p}}$. □

Theorem 6.3. *Let k, I, R be as in 6.2 and further assume that I is locally generated by a regular sequence of length t at every prime containing I. Then ϕ is injective.*

Proof : It is enough to show that $\phi_w p$ is injective for $\mathfrak{p} \supset I$. $(I/I^2)_{\mathfrak{p}}$ is $(R/I)_{\mathfrak{p}}$-free of rank t by 5.1. Since $K_{\mathfrak{p}}$is a homomorphic image of $(I/I^2)_{\mathfrak{p}}$, then $\mu(K_{\mathfrak{p}}) \leqslant t$. But rk $K_{\mathfrak{p}} =$ ht $I_{\mathfrak{p}} = t$ by 6.2. Thus $t =$ rk $K_{\mathfrak{p}} \leqslant \mu(K_{\mathfrak{p}}) \leqslant t$, so $K_{\mathfrak{p}}$ is free of rk t by 3.5 as R/I is reduced. Hence $\phi_{\mathfrak{p}}$ is injective. □

If k is perfect, then any extension is separably generated and hence we have :

Corollary 6.4. *ϕ is injective if k is a perfect field and I is a radical ideal of $R = k[X_1, \dots, X_n]$ s.t. I is locally generated by a regular sequence at every prime containing I.*

6.3 Fitting ideals and Jacobian ideal

Let M be a f.g R-module. Choose any finite set of generators $a_1, \dots, a_n$ and map $e_i \in R^n$ to a_i. We have a s.e.s $0 \to K \to R^n \to M \to 0$,with K being the kernel. We can think elements of K as elements of R^n. Form the matrix (K) where the rows are these n-tuples. The ***i*th Fitting ideal** $F_i(M)$ is defined to be the ideal generated by the determinants of all the $(n-i) \times (n-i)$ minors of (K), for $i = 0, 1, \dots, n-1$ and $F_i(M) = R$ if $i \geqslant n$.
Clearly, we could as well restrict the rows of (K) to a spanning set of K. These $F_i(M)$ are well-defined and invariant of the presentation of M. To show this, notice that it suffices to show that the F_i's got by the generating set $a_1, a_2, \dots, a_n$ and that obtained when an additional generator b is added are same, for then we can compare the F_i's got by $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_m$ by comparing both to that got by $a_1, \dots, a_n, b_1, \dots, b_m$.
So suppose b is an additional generator and $t_1 a_1 + \dots + t_n a_n + b = 0$. Then the new matrix is just the old matrix augmented with zeroes at the end and with an additional row $(t_1 \, \dots \, t_n \, -1)$. It is easily seen that the corresponding $F_i(M)$'s are same. Thus $F_i(M)$'s are well-defined. Also, $F_i(M_S) = F_i(M)R_S$.

1. For $\mathfrak{p} \in$ Spec$R$, $\mu(M_{\mathfrak{p}}) = \inf\{i|F_{i-1}(M) \subset \mathfrak{p}$ and $F_i(M) \not\subset \mathfrak{p}\}$. If $\mu(M_{\mathfrak{p}}) = n \geqslant 1$, then resolve $M_{\mathfrak{p}} : 0 \to K \to R_{\mathfrak{p}}^n \to M_{\mathfrak{p}} \to 0$. Then (K) has entries in $\mathfrak{p}R_{\mathfrak{p}}$ as $n = \mu(M_{\mathfrak{p}})$. So $F_{n-1}(M_{\mathfrak{p}}) \subset \mathfrak{p}R_{\mathfrak{p}}$ and $F_n(M_{\mathfrak{p}}) = F_n(M)_{\mathfrak{p}}$. Thus $F_{n-1}(M) \subset \mathfrak{p}$ and $F_n(M) \not\subset \mathfrak{p}$. Further, if $\mu(M_{\mathfrak{p}}) = 0$ then $M_{\mathfrak{p}} = 0$ and $R_{\mathfrak{p}} = F_0(M_{\mathfrak{p}}) = F_0(M)_{\mathfrak{p}}$, whence $F_0(M) \not\subset \mathfrak{p}$.

2. $F_0(M) = R$ iff $F_0(M_{\mathfrak{p}}) = R_{\mathfrak{p}}$ for $\mathfrak{p} \in$ Spec$R$ iff $\mu(M_{\mathfrak{p}}) = 0$ iff $M_{\mathfrak{p}} = 0$ iff $M = 0$.

3. $M_{\mathfrak{p}}$ is free of rank n iff $F_{n-1}(M_{\mathfrak{p}}) = 0$ and $F_n(M_{\mathfrak{p}}) = R_{\mathfrak{p}}$. This is clear as $F_{n-1}(M_{\mathfrak{p}}) = 0$ iff $(K) = 0$ i.e., $K = 0$.

4. $F(M) : 0 = F_0 = \dots = F_{\underline{r}-1} < F_{\underline{r}} \subset \dots \subset F_{\overline{r}-1} < F_{\overline{r}} = \dots = R$.

We will call $\underline{r}$ the **lower rank** of M and $\overline{r}$ the **upper rank** of M. For R reduced, $\underline{r}=\inf\{\mu(M_\mathfrak{p})|\mathfrak{p} \in \text{Spec } R\} = \text{rk } M$. This follows using the facts (i) $\mu(M_\mathfrak{p}) \geqslant \underline{r}$ (localize $F(M)$ at $\mathfrak{p}$) (ii) if equality doesn't hold, then $F_{\underline{r}}(M_\mathfrak{p}) \neq R_\mathfrak{p} \Rightarrow F_{\underline{r}}(M) \subseteq \mathfrak{p} \Rightarrow F_{\underline{r}}(M) \subset \sqrt{(0)} = (0)$ gives a contradiction. One similarly has that $\overline{r} = \sup\{\mu(M_\mathfrak{p})|\mathfrak{p} \in \text{Spec}R\}$.

Now let k be a field and $R = k[X_1, \ldots, X_n]$, we have the following presentation : $0 \to K \to (R/I)^n \to \Omega_k(R/I) \to 0$, and when $I = (f_1, \ldots, f_m)$, then (K) is just $\mathcal{J}(f_i; x)$.
Since $\underline{r}$ is the first non-zero Fitting ideal of $\Omega_k(R/I)$, rank $\mathcal{J}(f_i; x) = n - \underline{r}$. This also proves the fact the rank of $\mathcal{J}$ is independent of the generators chosen for I. $F_{\underline{r}}(\Omega_k(R/I))$ is called the **Jacobian ideal** of R/I and denoted by $\mathcal{J}(R/I)$.
Let $\mathfrak{p}$ be a prime in R/I and call $(R/I)_\mathfrak{p}$ **geometrically regular** if rank of $\mathcal{J}(f_i; x)$ doesn't decrease modulo $\mathfrak{p}$ or equivalently, by the discussion above, if $\mathcal{J}(R/I) \not\subset \mathfrak{p}$. R/I will be called **geometrically regular** if $(R/I)_\mathfrak{p}$ is for $\mathfrak{p} \in \text{Spec}R/I$.
Property 3 and 4 gives us that $(R/I)_\mathfrak{p}$ is geometrically regular iff $\Omega_k(R/I)_\mathfrak{p}$ is free of rank $\underline{r}$. Putting it all together,

Proposition 6.5. *Let k, R, I be as before with k perfect, I unmixed and radical and $\mathfrak{p} \in$ Spec R/I. The following are equivalent :*
(i) $(R/I)_\mathfrak{p}$ is geometrically regular
(ii) $\mathcal{J}(R/I) \not\subset \mathfrak{p}$
(iii) $\Omega_k(R/I)_\mathfrak{p}$ is free of rank $\underline{r}$.

To say this in a different way, we have that R/I is geometrically regular (with the necessary hypothesis) iff $\Omega_k(R/I)$ is projective of constant rank $\underline{r}$. We shall see in the next section that the notion of geometrical regularity coincides with that of regularity when k is perfect. Assuming this for the moment, we have that for an ideal I of $R = k[X_1, \ldots, X_n]$ s.t. I is unmixed and R/I is regular, $\Omega_k(R/I)$ is a f.g. R/I-projective of constant rank $\underline{r}$. Thus the sequence

$$0 \to I/I^2 \xrightarrow{\phi} (R/I)^n \xrightarrow{D\pi} \Omega_k(R/I) \to 0$$

splits, thereby giving $(I/I^2) \oplus \Omega_k(R/I) \cong (R/I)^n$.

6.4 Jacobian criteria for regularity

Eisenbud ?? doubts in cor

6.5 Rational curves

A large class of non-singular curves are known to have cyclic module of differentials and hence are complete intersection. We shall prove here that irreducible non-singular space curves of genus 0 is one such class. In this respect, we will begin with the characterization that a irreducible non-singular curve is of genus 0 iff the quotient field of its affine ring is the field of rational functions in one variable, or a simple transcendental extension. Such curves are also called **rational curves**. The following result shows that $\Omega_k(R/I)$ is a free module of rk 1 and hence I is a complete intersections.

Proposition 6.6. *Let k be an algebraically closed field and $k(t)$ be a simple transcendental extension. Then for D, a domain s.t. $k \subsetneq D \subset k(t)$, $\Omega_k(D)$ is free of rk 1 and D is a PID.*

Proof: All the valuations of $k(t)$ containing k are the $1/t$-adic (the ∞ valuation) and the p-adic where p corresponds to an irreducible polynomial in $k[t]$, and since k is alg. closed, the only irreducible

polynomials are the linear ones, i.e., $(t-\alpha)$, $\alpha \in k$. Since D is integrally closed, by 9.4, D is the intersection of all such valuations containing it. But one such valuation is excluded from this intersection as k is the intersection of all such and $k \subsetneq D$. If the p-adic (=$1/t$ or $t-\alpha$) is excluded, then it is in all other valuations and hence is in D. Thus, by replacing t in $k(t)$ by $1/p$ if necessary, we may assume $k[t] \subset D$.
Put $S = \{f \in k[t] \mid 1/f \in D\}$. We claim that $D = k[t]_S$. Let $a \neq 0$ belong to D and $a = f/g$, $f, g \in k[t]$ s.t. a is in reduced form, i.e., $(f,g) = k[t]$. Then $1 = pf + qg$, $p, q \in k[t]$, whence $1/g = pa + q \in D$.
Now it is clear that every ideal of D is an extended ideal of $k[t]$, which is a PID, hence so is D. Similarly, $\Omega_k(D) = \Omega_k(k[t]_S) = \Omega_k(k[t])_S$ is rk 1 free. □

7 Set-theoretic complete intersection

Recall that an ideal I in $R = k[X_1, X_2, \dots, X_n]$ is called **set-theoretic complete intersection** if there is an ideal J s.t. $\sqrt{J} = I$ and $\mu(J) = \text{ht } I$. What we will prove is :
Theorem 7.1. *Let I be the defining ideal of a non-singular, irreducible space curve, i.e., in $R = k[X_1, X_2, X_3]$, k alg. closed. Then I is a set-theoretic c.i.*

Proof: We trace the outline of steps we'll proceed on : find an ideal J s.t. $I^2 \subset J \subset I$, J is local c.i. of ht 2 and J/J^2 is R/J-free of rk 2. Then by §5, $\Omega_k(R/J) \cong \text{Ext}^1_R(J, R)$ is free of rk 1 and by 3.3, J is a c.i. ideal.
The co-ordinate R/I is a Dedekind domain (clear as it is Noetherian of dim 1; int. closed follows from Euclid's algorithm on R). Then from 9.12, we have that a f.g. R/I-projective is free if its **determinant** (maximal exterior power) is free.
We already have that I/I^2 is a projective of rk 2 and $\Omega_k(R/I)$ is a projective of rk 1. By 9.14, $\Omega_k(R/I)$ is direct summand of I/I^2 and thus we can choose a surjection $I/I^2 \overset{\phi}{\twoheadrightarrow} \Omega_k(R/I)$. Let J be the kernel. Then $I^2 \subset J \subset I$, $\sqrt{J} = I$ and ht $J = 2$. Locally, we can choose generators a, b of I/I^2 s.t. ϕ sends a to zero. Then J is generated by a and (a^2, b^2), i.e., generated by a, b^2. Thus J is a local c.i. of ht 2 and so J/J^2 is a projective of rk 2.
To show that J/J^2 is free, it suffices to show that it is generated by 2 elements for then, locally its direct summand of $(R/J)^2$ is zero, whence zero. Since $(I/J)^2 = 0$ in R/J, I/J is in the Jacobson radical of R/J and hence by Nakayama, $\mu(J/J^2) = \mu(J/J^2 \otimes_{R/J} (R/J)/(I/J)) = \mu(J/IJ)$. We have to show $\mu(J/IJ) = 2$. But $J/IJ = J \otimes_R R/I = J \otimes_R R/J \otimes_{R/J} \otimes R/I = J/J^2 \otimes_{R/J} R/I$ is a R/I-projective of rk 2. By 9.12, to show that J/IJ is free of rk 2 it is enough to show that $\wedge^2 J/IJ \cong R/I$. Now the following s.e.s.

$$0 \to I^2/IJ \to J/IJ \to J/I^2 \to 0$$

has rk $(J/I^2) = 1$ and rk $(I^2/IJ) = 1$ and on taking exterior powers, $\wedge^2(J/IJ) = J/I^2 \otimes_{R/I} I^2/IJ$. By the construction of J, $I/J \cong \Omega_k(R/I) \cong \text{Hom}_{R/I}(\bigwedge^2(I/I^2), R/I)$ and $\bigwedge^2(I/I^2) = \Omega_k(R/I)^*$. But $\bigwedge^2(I/I^2) = J/I^2 \otimes_{R/I} \Omega_k(R/I)$ as J/I^2 is projective of rk 1. On tensoring this with $\Omega_k(R/I)^*$, we have $J/I^2 = \Omega_k(R/I)^{*\otimes 2}$. Also, since there is the usual (bilinear) map from $I/J \times I/J$ to I^2/IJ, it factors through $(I/J)^{\otimes 2}$. This map is locally an isomorphism as I/J is locally free of rk 1 and so is I^2/IJ, whence it is an isomorphism. Thus $I^2/IJ = \Omega_k(R/I)^{\otimes 2}$. Putting all these together, we see that $\wedge^2(J/IJ) \cong R/I$ by 9.13. Thus J/IJ is free and we're done. □

8 Cowsik-Nori Theorem

We provide a proof of the theorem of Cowsik-Nori titled "Curves in characteristic p are set-theoretic complete intersections". Towards proving it, we require some preparatory results. Fix throughout, a prime number p and a field k of characteristic p.

8.1 A projection lemma

What we shall roughly prove is that a curve C in n-space can be projected into a plane in a way so as to map C isomorphically to its image except possibly for a finite set of points.

Definition 8.1. An injective homomorphism $A \to B$ of reduced Noetherian rings is called **birational**, if it induces an isomorphism of the total quotient rings.

Proposition 8.2 (Projection Lemma)**.** *Let I be unmixed, ht $n-1$ radical ideal of $R = k[X_1, \ldots, X_n]$. Then by a change of variables, the ring extension $k[X_1, X_2]/(k[X_1, X_2] \cap I) \hookrightarrow R/I$ is finite and birational.*

The proof requires some further preparations.

Lemma 8.3. *Let $k[X, Y]$ be the polynomial ring in two variables over a perfect field k of charactersitic p and f be an irreducible polynomial. Then $\partial f/\partial X \neq 0$ or $\partial f/\partial Y \neq 0$.*

Proof: If $p = 0$ the assertion is clear. For $p \geqslant 1$, if both the partials are zero, then $f = g^p$ for some $g \in k[X, Y]$, contradicting the irreducibility of f. □

Lemma 8.4. *Let $k[X, Y]$ and f be as in Lemma 8.3. Then for large enough m s.t. $p \neq |m$, $f(X + Y^m, Y)$ is monic in Y and*

$$\partial f(X + Y^m, Y)/\partial Y \neq 0$$

Proof: For large enough m s.t. $p \not| m$, $F = f(X + Y^m, Y)$ is monic (upto a unit) in Y. Also,

$$\frac{\partial F}{\partial Y} = mY^{m-1}\frac{\partial f}{\partial X}(X + Y^m, Y) + \frac{\partial f}{\partial Y}(X + Y^m, Y)$$

If $\frac{\partial f}{\partial Y} \neq 0$ then $\frac{\partial f}{\partial Y} \neq\in (Y^r)$ for some r. Thus $\frac{\partial f}{\partial Y}(X + Y^m, Y)$ is not in (Y^r) for any m. In this case, choosing $m > r$ we have that the first term of the RHS belong to (Y^r) but the second term doesn't, whence $\frac{\partial F}{\partial Y} \neq 0$.
If $\frac{\partial f}{\partial Y} = 0$, then by 8.3 $\frac{\partial f}{\partial X} \neq 0$. Thus if $p \not| m$, we have $\frac{\partial F}{\partial Y} \neq 0$. □

Lemma 8.5. *Let K be a finite field extension of k, any field with $K = k(y, z)$. If y is separable over k, then $K = k(cy + z)$ for all but finitely many $c \in k$.*

Proof: blah blah □

Lemma 8.6. *Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be two distinct maximal ideals of $k[X, Y]$. Then $\mathfrak{p}_1 \cap k[X+cY] \neq \mathfrak{p}_2 \cap k[X+cY]$ for all but finitely many c in k.*

Proof: Let L be the algebraic closure of k and □
Proof of Proposition : blah blah □

8.2 The theorem of Cowsik and Nori

We require the following :

Definition 8.7. Let $A \subset B$ be a ring extension. The **conductor** $\mathfrak{c}$ of this extension is defined by $\mathfrak{c} := Ann_A(B/A)$.

REMARKS : (a) The conductor $\mathfrak{c}$ is an ideal of B contained in A.
(b) If it is a birational finite extension of reduced rings, then take any finite generating set for B over A, say $x_1, \ldots, x_n$. As the quotient rings are isomorphic, $x_i/1$'s can be identified with elements of the quotient ring of A, with a comon denominator s. Then s lies in $\mathfrak{c}$ and is a non-zero divisor.

Theorem 8.8. *Every curve in affine n-space over a field k of characteristic $p > 0$ is a set-theoretic complete intersection.*

Proof : blah blah □
Bortyanski's thm

9 A few loose ends!

As the saying goes,

A few stray threads, hanging loose albeit!
Knit it to a whole to make it complete!

9.1 Cohen-Macaulay rings and grade

A ring R is called **Cohen Macaulay** if ht $\mathfrak{m} = G(\mathfrak{m})$ for any maximal ideal $\mathfrak{m}$ of R, where $G(\mathfrak{m})$ denotes the grade of $\mathfrak{m}$. This implies $G(I) =$ ht I for any ideal I. For a proof of this and related properties refer [2] pgs 95-100. For our purpose, $R = k[X_1, \ldots, X_n]$ is a CM ring and any localization of it is also CM.
Coming to grades, we finally prove that grade is well-defined. For that we require some results :

Lemma 9.1. *Let C, D be R-modules. Suppose there is an element $x \in R$ s.t. $x\ C = 0$ and $x \notin \mathcal{D}$. Then $Hom_R(C, D) = 0$.*

Proof : Let $f \in \mathrm{Hom}_R(C, D)$. $f(xc) = 0$ for $c \in C$ implies that $f(c) = 0$, whence $f = 0$. □

Proposition 9.2. *Let A, B be R-modules. Assume that $x_1, \ldots, x_n \in R$ is an R-sequence on A and $(x_1, \ldots, x_n)B = 0$. Then $Ext^n_R(B, A) \cong Hom_R(B, A/(x_1, \ldots, x_n)A)$.*

Proof : We proceed by induction on n. For $n = 1$, since x_1 is a non-zero-divisor on A, $0 \to A \stackrel{x_1}{\to} A \to A/x_1A \to 0$ is exact. So $\mathrm{Hom}_R(B, A) \to \mathrm{Hom}_R(B, A/x_1A) \to \mathrm{Ext}^1_R(B, A) \stackrel{x_1}{\to} \mathrm{Ext}^1_R(B, A)$ is exact with $\mathrm{Hom}_R(B, A) = 0$ by the previous lemma, and image of $\mathrm{Ext}^1_R(B, A)$ under x_1 being zero as $x_1B = 0$. Hence the result holds for $n = 1$.
For $n > 1$, we have $\cdots \to \mathrm{Ext}^{n-1}_R(B, A) \to \mathrm{Ext}^{n-1}_R(B, A/x_1A) \to \mathrm{Ext}^n_R(B, A) \stackrel{x_1}{\to} \mathrm{Ext}^n_R(B, A) \to \cdots$. But $\mathrm{Ext}^{n-1}_R(B, A) \cong \mathrm{Hom}_R(B, A/(x_1, \ldots, x_{n-1})A) = 0$ by induction hypothesis and lemma with $x = x_n$. Also image of $\mathrm{Ext}^n_R(B, A)$ under x_1 is zero. Hence $\mathrm{Ext}^n_R(B, A) \cong \mathrm{Ext}^{n-1}_R(B, A/x_1A) \cong \mathrm{Hom}_R(B, A/(x_1, \ldots, x_n)A)$. □

Theorem 9.3. *$G_R(I) = inf\ \{n \mid Ext^n_R(R/I, R) \neq 0\}$.*

Proof : Take $B = R/I$ and $A = R$ in the result above. Then $\mathrm{Hom}_R(R/I, R/(x_1, \ldots, x_n)) \neq 0$ iff there is a non-zero r in $R/(x_1, \ldots, x_n)$ s.t. $rI = 0$ in $R/(x_1, \ldots, x_n)$. This is seen by taking $r = \phi(1)$ for any non-zero element ϕ in $\mathrm{Hom}_R(R/I, R/(x_1, \ldots, x_n))$ and noting that I is in the kernel. Now $rI = 0$ with r as before happens iff $I \subset \mathcal{Z}(R/(x_1, \ldots, x_n))$. Again, the "only if" part is clear. The "if" part follows from the fact that the set of zero-divisors of a f.g. module M is a finite union of prime ideals, each annihilating an element of M and Prime Avoidance lemma.
Thus, we see that $x_1, \ldots, x_n$ is a maximal R-sequence in I. Hence, we can characterize $G_R(I)$ as being $\inf\ \{n \mid \mathrm{Ext}^n_R(R/I, R) \neq 0\}$. □

9.2 Projective dimension

Let N be a R-module. An exact sequence $0 \to P_n \to \cdots \to P_0 \to N \to 0$ with P_i's f.g. projective is called a **projective resolution** of length n for N. A f.g. projective resolution of length ∞ is defined similarly. For any N having such a resolution, the **f.g. projective dimension** is defined by $d(N) = \inf\{n|N$ has a f.g. projective resolution of length $n\}$.
To define projective dimension for a module, we need a equivalence relation and a lemma :

Definition 9.4. Two modules M_1, M_2 are said to be **projectively equivalent** if there exists projective modules P_1, P_2 s.t. $P_1 \oplus M_1 \cong P_2 \oplus M_2$.

Lemma 9.5 (Schanuel's Lemma)**.** *Let $0 \to K_1 \to P_1 \to M \to 0$ and $0 \to K_2 \to P_2 \to M \to 0$ exact sequences with P_1, P_2 projective. Then $K_1 \oplus P_2 \cong K_2 \oplus P_1$.*

Proof : We have the following commutative diagram below

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 & \longrightarrow & P_1 & \xrightarrow{f_1} & M & \longrightarrow & 0 \\ & & & & \big\downarrow g & & \big\downarrow id & & \\ 0 & \longrightarrow & K_2 & \longrightarrow & P_2 & \xrightarrow{f_2} & M & \longrightarrow & 0 \end{array}$$

where the map g exists as P_1 is projective. Define L to be the kernel of $\phi : P_1 \oplus P_2 \to M$ sending (x, y) to $f_1(x) - f_2(y)$. We shall show that $P_1 \oplus K_2 \cong L$. A similar reasoning will then show that $P_2 \oplus K_1 \cong L$ and we'll be done. We define a map $\psi : P_1 \oplus K_2 \to L$ by $(p, k) \mapsto (p, g(p) + k)$. Then it is clear that this is well-defined (i.e., lands (p, k) in L) and is surjective as if $(p, p') \in L$, then $f_2(p') = f_1(p) = f_2(g(p))$, whence $p' = g(p) + k$ with $k \in K_2$. Injectivity of ψ is clear. □

Corollary 9.6. *Let $0 \to K \to P_n \to \cdots \to P_0 \to M \to 0$ and $0 \to L \to Q_n \to \cdots \to Q_0 \to M \to 0$ be two exact sequences with Q_i, P_i's projective. Then*

$$K \oplus Q_n \oplus P_{n-1} \oplus Q_{n-2} \cdots \cong L \oplus P_n \oplus Q_{n-1} \oplus P_{n-2} \oplus \cdots .$$

Proof : The proof proceeds by induction on n, the case $n = 1$ being Schanuel's Lemma. For $n > 1$, let $K_0 = ker(P_0 \to M)$ and $L_0 = ker(Q_0 \to M)$. Then the s.e.s $0 \to K_0 \to P_0 \to M \to 0$ (corres. for L_0) gives $L_0 \oplus P_0 \cong K_0 \oplus Q_0$. One has the exact sequences

$$\begin{array}{c} 0 \to K \to P_n \to \cdots \to P_1 \to K_0 \to 0 \\ 0 \to L \to Q_n \to \cdots \to Q_1 \to L_0 \to 0 \end{array}$$

which gives rise to

$$0 \to K \to P_n \to \cdots \to P_2 \to P_1 \oplus Q_0 \to K_0 \oplus Q_0 \to 0$$
$$0 \to L \to Q_n \to \cdots \to Q_2 \to Q_1 \oplus P_0 \to L_0 \oplus P_0 \to 0$$

By induction hypothesis, the above gives the required isomorphism. □

It follows form 9.6 that if $d(N) \leqslant n$ and $0 \to K \to P_n \to \cdots \to P_0 \to N \to 0$ is exact with P_i's f.g. projective, then so is K.
If one has a s.e.s $0 \to K \to P \to M \to 0$ with P projective, then by Schanuel's Lemma, K is uniquely determined upto projective equivalence and can be denoted by $\mathcal{R}M$. Now repeat the same with K in place of M and denote the resulting module, again upto projective equivalence, by $\mathcal{R}^2M$. The **projective dimension** of M is defined to be the smallest such n for which $\mathcal{R}^nM$ is the class of projective modules.
For any Noetherian ring R, the notions of f.g. projective dimension and projective dimension coincide for a f.g. module. For, if projective dimension $\leqslant n$ then we have exact sequences for $i = 0, \ldots, n-1$:

$$0 \to \mathcal{R}^{i+1}N \xrightarrow{\psi_{i+1}} Q_{i+1} \xrightarrow{\varphi_{i+1}} \mathcal{R}^iN \to 0.$$

By construction Q_i's are projective. Since R is Noetherian, can take Q_1 to be f.g. whence $\mathcal{R}N$ and consequently all the Q_i's are f.g. A simple calculation verifies that the sequence

$$0 \to \mathcal{R}^nN \xrightarrow{\psi_n} Q_n \xrightarrow{\psi_{n-1}\circ\varphi_n} Q_{n-1} \to \cdots \to Q_1 \xrightarrow{\varphi_1} N \to 0$$

is exact. Hence $d(N) \leqslant n$. Conversely, if $d(N) \leqslant n$, then by breaking up the f.g. projective resolution of N into s.e.s(s), we have projective dimension $\leqslant n$.
lemma p.d=non-vanishing of Ext
lemma dN d=sup
lemma for R Noetherian

9.3 Projective modules

In this part we supply proofs of f.g. projectives over a local ring being free, a well-known structure theorem for f.g. projectives over a Dedekind domain and an easy lemma on modules over Artinian local rings.

Lemma 9.7. *Let R be a local ring and P a f.g. R-projective. Then P is free.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of R and let $k = R/\mathfrak{m}$. Then any set of generators $\{x_1, \ldots, x_n\}$ of $P/\mathfrak{m}P$ as a k-vector space is also a generating set for P over R. Thus one has an exact sequence $0 \to Q \to R^n \xrightarrow{\phi} P \to 0$ with ϕ mapping e_i to x_i. Because P is projective, this sequence splits and hence on tensoring with k, the resulting sequence $0 \to k \otimes_R Q \to k^n \xrightarrow{1\otimes\phi} k \otimes_R P \to 0$ is split exact. By construction, $1 \otimes \phi$ is an isomorphism. Hence $Q/\mathfrak{m}Q = k \otimes_R Q = 0$, whence by Nakayama's lemma $Q = 0$. □

Lemma 9.8. *Let R be an Artinian local ring and M be a R-module s.t. there is a s.e.s $0 \to R^m \to R^n \to M \to 0$. Then M is free.*

Before beginning the proof let us digress a little. Let $R, \mathfrak{m}$ be a local ring and let M, N be a f.g. module over R. If $\varphi : M \to N$ is a R-module homomorphism then $\overline{\varphi}$ will denote the induced map $M \otimes_R k \to N \otimes_R k$, where $k = R/\mathfrak{m}$. An exact sequence

$$\cdots \to F_i \overset{\phi_i}{\to} F_{i-1}\phi_{i-1}\to \cdots \to F_1 \overset{\phi_1}{\to} F_0 \overset{\varepsilon}{\to} M \to 0$$

is called a **minimal free resolution** of M if (i) each F_i is R-free (ii) $\overline{d_i} = 0$ i.e., $d_iF_i \subset \mathfrak{m}F_{i-1}$ and (iii) $\overline{\varepsilon}$ is an isomorphism. For M, a f.g. module over R Noetherian local, a minimal resolution always exist. Let $\{x_1, \ldots, x_n\}$ be a minimal basis of M and let F_0 be the free module $Rx_1 + \cdots + Rx_n$. Define ε by $\varepsilon(e_i) = x_i$; then $\overline{\varepsilon} = 0$. Let K_1 be the kernel. Now K_1 is again a f.g. module and we proceed as before. It is known that any two minimal free resolutions of M are isomorphic as complexes.

Proof : By the discussion above we can assume the given s.e.s $0 \to R^s \overset{\phi}{\to} R^t \to M \to 0$ to be a free minimal resolution of M. Since R is Artinian local, $\mathfrak{m}$ is the nilradical and hence nilpotent. Let $t \geqslant 0$ be the smallest integer s.t. $\mathfrak{m}^t = 0$. Note that this implies there is a non-zero $s \in \mathfrak{m}^{t-1}$. This s annihilates every element of $\mathfrak{m}$. The map ϕ can be thought of as a matrix with entries in $\mathfrak{m}$, and this involves only finitely many elements of $\mathfrak{m}$. Hence, s annihilates R^s, whence $R^s = 0$. Thus M is free. □

The next string of results will assume R to be a Dedekind domain. We will also assume certain basic properties of such rings.

Lemma 9.9. *Let $M \subset R^n$ be a submodule with R, a Dedekind domain. Then M is the direct sum of at most n rk 1 R-projectives.*

Proof : We induct on n, the statement being clearly true for $n = 1$ as any ideal is a rk 1 projective. For $n > 1$, let π_n be the projection onto the last factor and let R^{n-1} denote its kernel. This gives us an exact sequence

$$0 \to M \cap R^{n-1} \to M \to \pi_n(M) \to 0.$$

Since $\pi_n(M)$ is an ideal (hence projective), this sequence splits. Thus $M \cong (M \cap R^{n-1}) \oplus \pi_n(M)$ and by the induction hypothesis we're through. □

As a result, we have that every (f.g.) projective is a direct sum of (ideals) rk 1 projectives.

Proposition 9.10. *Let P, Q be rk 1 R-projectives. Then $P \oplus Q \cong (P \otimes_R Q) \oplus R$.*

Proof : P and Q are isomorphic to invertible ideals I and J resp. of R. We claim that there is an ideal $I' \cong I$ s.t. $I' + J = R$. Once we have this, then the map $\psi : I' \oplus J \to R$ defined by $\psi(x, y) = x - y$ is surjective with the kernel being $I' \cap J = I'J$ by the Chinese Remainder theorem. Hence, the exact sequence $0 \to I' \cap J \to I' \oplus J \overset{\psi}{\to} R \to 0$ splits, whence $I' \oplus J \cong I'J \oplus R$. But $I'J \cong P \otimes_R Q$ by property (a) of 5.5. So $(P \otimes_R Q) \oplus R \cong P \oplus Q$.
By factorization of J into prime ideals, only finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ contain J. Set $S = R \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i$. Then $S^{-1}(I^{-1})$ is an invertible fractional ideal of $S^{-1}R$. Since $S^{-1}R$ is semi-local, $S^{-1}(I^{-1})$ is free of rk 1, i.e., principal (cf 4.1). Let z^{-1} be a generator and put $I' = zI$. Then $S^{-1}I' = S^{-1}R$ and hence I' is not contained in any of the $\mathfrak{p}_i$'s. Thus $I' + J = R$. □

As an upshot of all this, we have :

Theorem 9.11. *Any f.g. projective module P of rk n over a Dedekind domain R is of the form $P = R^{n-1} \oplus L$, where L is a rk 1 projective module.*

Proof : This is clear after writing P as a direct sum of n rk 1 projectives (by 9.9) and using 9.10 repeatedly. □

Corollary 9.12. *A f.g. projective R-module P is free iff its determinant is free.*

Proof: Write $P = R^{n-1} \oplus L$ with L a rk 1 projective, as before. Then $\det(P) \cong \wedge^{n-1} R^{n-1} \otimes_R L$. So the determinant is free implies that L is free, whence P is! The other side implication is obvious. □
We shall state and prove two further results needed in 7.1

Lemma 9.13. *Let L be a R-projective of rk 1 and let $L^* = Hom_R(L, R)$. Then $L \otimes_R L^* \cong R$.*

Proof: Define $\phi : L \times L^* \to R$ by $\phi(f, g) = g(f)$. This induces a map $\overline{\phi} : L \otimes_R L^* \to R$. $\overline{\phi}_{\mathfrak{p}}$ is an isomorphism for $\mathfrak{p} \in \mathrm{Spec}R$, whence $\overline{\phi}$ is. □

Lemma 9.14. *Let P be a f.g. R-projective of rk $r \geqslant 2$. Then every rk 1 R-projective Q is a direct summand of P.*

Proof: We already have $P \cong R^{r-1} \oplus P'$. Then $R^{r-2} \oplus (P' \otimes_R Q^*) \oplus Q \cong R^{r-2} \oplus (P' \otimes_R Q^* \otimes_R Q) \oplus R \cong R^{r-1} \oplus P'$. □

9.4 Valuations

We assume the definitions of a valuation ring and valuations (cf [1] pgs. 251-252). Further, we assume certain properties (easily verified) like a valuation ring being integrally closed in its quotient field and that a ring R is a valuation ring iff R is a domain s.t. either x or x^{-1} is in R for x in the quotient field $K(R)$. We also note that for any domain R, $r \in K(R)$, r^{-1} is integral over R iff $rR[r] = R[r]$ iff $r^{-1} \in R[r]$ (follows from writing down the equation of r^{-1}).
Let R be any domain and $\mathfrak{p} \subset R$ be a prime ideal. By Zorn's lemma there is R', subring of $K(R)$ containing R and maximal w.r.t the property that $\mathfrak{p}R' \neq R'$. This is clear as for any chain with the usual partial order, the union is the upper bound and it satisfies the stated property.
$R' \subset R'_{\mathfrak{p}}$ and $\mathfrak{p}R'_{\mathfrak{p}} \neq R'_{\mathfrak{p}}$; hence by the maximality of R' w.r.t $\mathfrak{p}$, $R' = R'_{\mathfrak{p}}$, implying that R' is local. Now $R' \subset \overline{R'}$ and by the going-up theorem there is a prime $\overline{\mathfrak{p}}$ in $\overline{R'}$ s.t. $\overline{\mathfrak{p}} \cap R' = \mathfrak{p}$. Thus $\mathfrak{p}\overline{R'} \neq \overline{R'}$. Again, as before, $R' = \overline{R'}$. Notice that since $R \setminus \mathfrak{p} \subset R' \setminus \mathfrak{p}$, $R_{\mathfrak{p}} \subset R'_{\mathfrak{p}} = R'$. The maximal ideal $\mathfrak{m}$ of R' is just $\mathfrak{p}R'_{\mathfrak{p}}$ and so $\mathfrak{m} \cap R = \mathfrak{p}$. If $x \notin R'$, then $x \notin R[x^{-1}]$ and hence x^{-1} (a non-unit) is in some maximal ideal $\mathfrak{m}'$ of $R'[x^{-1}]$. Now $\mathfrak{p}R'[x^{-1}] = \mathfrak{m}[x^{-1}] \subset \mathfrak{m}' \neq R'[x^{-1}]$. Hence $R' = R'[x^{-1}]$ and $x^{-1} \in R'$, making R' a valuation ring.
Once we have the existence of valuation rings containing R, we next show that the integral closure of R (denoted by $\overline{R}$)in its quotient field is the intersection of the valuation rings containing R. Since the intersection of integrally closed domains is again so, one side inclusion is clear. We need only show that if $x \notin \overline{R}$, then there is a valuation ring R' containing R s.t. $x \notin R'$. This would then give the other inclusion. Let $x \notin \overline{R}$. Then $x \notin R[x^{-1}]$, implying that x^{-1} is not a unit in $R[x^{-1}]$ and is contained in a maximal ideal $\mathfrak{m}$. As with the existence of valuation rings, let R' be (any one) maximal w.r.t all subrings of $K(R)$ containing $R[x^{-1}]$ s.t. $\mathfrak{m}$ doesn't extend to the whole subring. Then by the initial arguments, R' is a valuation ring and $x^{-1} \in \mathfrak{m} \subset \mathfrak{m}'$ where $\mathfrak{m}'$ is a maximal ideal of R'. Thus the valuation of x^{-1} w.r.t R' is strictly positive and hence the corresponding valuation of x is strictly negative, whence $x \notin R'$.

References

[1] D. Eisenbud, **Commutative Algebra** *with a View Toward Algebraic Geometry*, **150** Springer-Verlag GTM

[2] I. Kaplansky, *Commutative Rings*, Univ. of Chicgao Press

[3] S. Lang, *Algebra*, Addison-Wesley

[4] S. Mandal, *Projective Modules and Complete Intersections*, Springer **LNM** 1672

[5] Matsumura, *Commutative Rings*,

[6] J. Ohm, *Space-curves as Ideal-Theoretic Complete Intersections*, Studies in Math MAA **20** 47-115

[7] R.G. Swan, *The number of generators of a module*, Math. Z. **102** 318-322