Five lectures on Computational Commutative Algebra Introduction to W. Decker's Workshop at H.R.I. January 2-11, 2003.

Ravi A. Rao
School of Mathematics, Tata Institute of Fundamental Research,
Homi Bhabha Road, Mumbai 400 005.

1 Solving Polynomial Equations

Gröbner Bases

Solving systems of algebraic equations is one of the most challenging problems of Algebra, and the computational complexity makes it a challenge for Computer Algebra.

The problem: Given a system of polynomial equations $f_1 = 0, f_2 = 0, \cdots, f_k = 0$, where $f_i \in D[x_1, \cdots, x_n]$, for some domain D, we search for all solutions $(z_1, \cdots, z_n) \in \overline{D}^n$, where $\overline{D}$ denotes the algebraic closure of the quotient field of D. Typically, $D = \mathbf{Z}$, the ring of integers.

If two sets of polynomials generate the same ideal, or generate ideals having the same radical ideal, they will have the same solutions. The *Hilbert's Nullstellensätz* asserts that the converse is true: two sets of system of polynomial equations have the same set of solutions iff the ideal they generate have the same radical. Thus, one can associate an affine algebra with the set of solutions.

The set of solutions is a subset of affine subset $\overline{D}^n$, and is called an *algebraic set*. These sets form the closed set of the *Zariski topology* on $\overline{D}^n$. An algebraic set which is not the union of two smaller ones is irreducible, and any algebraic set is a finite union of irreducible one (called components), and this decomposition is unique. Algebraically, this is the well-known *Lasker-Noether* primary decomposition of an ideal in a polynomial ring over a field.

The dimension of the set of solutions is the dimension of the affine algebra associated to it, which happens to be the maximal dimension of its components. For a component, the dimension works out to be the transcendence degree of the quotient field of the associated affine domain. Thus, the dimension is 0 for a finite set of points, 1 for a curve, 2 for a surface, etc. A system has dimension 0 iff it has a finite number of solutions.

The first effective algorithm for solving algebraic equations is the *Buchberger's algorithm* for computing Gröbner bases. A Gröbner bases $G = \{g_1, \cdots, g_r\}$ is essentially a set of generators of an ideal $(f_1, \cdots, f_s)$, which permits an exact division algorithm: $f \in (f_1, \cdots, f_s)$ iff its division by $g_1, \cdots, g_s$, will have remainder zero. Equivalently, a set of generators of an ideal $I = \{f_1, \cdots, f_s\}$ such that their leading coefficients $\{L(f_1), \cdots, L(f_s)\}$ generate the leading coefficient ideal $L(I)$, which is the ideal generated by all leading coefficients of elements of I. The algorithm shows how to get such a bases.

This algorithm, which generalizes Gaussian elimination, is the most efficiently implemented algorithm. Under additional hypothesis, one can assert that the bases is unique - it is called the reduced Gröbner base, w.r.t. some monomial ordering. A set of equations will have an empty set of solution iff $\{1\}$ is a reduced Gröbner base for any monomial ordering. Equivalently, a system of equations is zero-dimensional iff there is a Gröbner base which contains for each x_i a polynomial with a power of x_i as its leading monomial. The geometrical dimension of the set of solution can be deduced from the leading monomials of a Gröbner base, as well as other invariants of the ideal, like the Hilbert polynomial.

We will discuss several approaches to solving systems of polynomial equations, based on the elimination properties of lexicographic Gröbner bases. Combining elimination with numerical root-finding for one variable polynomials we will demonstrate a conceptually simple method that generalizes the usual techniques used to solve sytems of linear equations: The Elimination theorem shows that a *lex* Gröbner basis G successively eliminates more and more variables. This gives the following strategy for finding all solutions of the system: start with the polynomials in G with the fewest variables, solve them, and then try to extend these partial solutions to solutions of the whole system, applying the Extension Theorem one variable at a time. This method works especially when the variety $V(I)$ is finite.

Gröbner bases theory provides the foundation for many algorithms in Algebraic Geometry & Commutative Algebra, with the Buchberger algorithm being the engine that drives the computations. We emphasize how to use Gröbner bases as a basic building block in designing more advanced algebraic algorithms, and to show how Gröbner bases can be used as a computational tool to prove a theorem or to disprove a conjecture or just to experiment with examples in order to obtain a feeling about, say, the structure of an algebraic variety.

Krull dimension of Semigroup Rings or Monomial subrings

They are subrings of the ring of Laurent polynomials

$$R = k[x_1,\ x_1^{-1}, \ldots, x_n,\ x_n^{-1}]$$

generated by a finite set of monomials $A = k[f_1, \ldots, f_m],\ f = x^a = x_1^{a_1} \cdots x_n^{a_n}$, $a = (a_1 \cdots a_n) \in \mathbf{Z}^n$. Each such ring is coded by the integral matrix whose rows are the exponent vectors a_i of the f_j's.

$$\varphi = \begin{pmatrix} a_1 \\ \vdots \\ a_q \end{pmatrix}$$

For ease of terminology we refer to the rows of φ as "vectors" or "monomials", and the ring is denoted $k[\varphi]$.

Proposition. Let φ be a matrix with integral entries. Then for any field k.

$$\dim k[\varphi] = \text{rank} \quad (\varphi).$$

Proof: We determine the Krull dimension of $A = k[\varphi] = k[f_1 \cdots f_q]$ as the transcendence degree of its field of fractions. To this end, note that effecting any elementary row operation (over the integers) on φ produces an integal matrix whose associated semigroup ring has the same transcendence degree. Carrying out full row reduction (possibly involving exchange of columns) leaves a matrix of the form

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & * & * \\ 0 & d_2 & \cdots & 0 & * & * \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_r & * & * \end{pmatrix}$$

with $d_1 \neq 0$, whose attached semigroup ring is generated by r algebraically independent elements.

Computing Krull dimension of Affine domains

In this section we give an algorithm, due to Kredel-Weispfenning to compute the Krull dimension of an affine domain.

The Algorithm. Let $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ be a prime ideal. Let G be a Gröbner base of $\mathfrak{p}$ with respect to a lexicographic order with $x_1 < x_2 < \cdots < x_n$. Let $T_0 = \emptyset$, and $0 < j \leq n$ let T_j be defined by

$$\begin{cases} T_{j-1} & \text{if } G \cap (k[x_1, \ldots, x_j] - k[x_1, \ldots, x_{j-1}]) \neq \emptyset \\ T_{j-1} \cup \{x_j\} & \text{otherwise} \end{cases}$$

Then height $\mathfrak{p} = \mid T_n \mid$. Moreover$\mathfrak{p} \cap k[T_n] \neq \emptyset$, i.e. T_n is algebraically dependent module $\mathfrak{p}$. (T_n will be denoted by $T_{\mathfrak{p}}$ below.)

To prove this algorithm we first prove

Lemma. Let $g \in k[x]$ be an irreducible polynomial, and let $f \in k[y_1, \ldots, y_d,\ x] \backslash (g)$. Then $(f,\ g) \cap k[y_1, \ldots, y_d] \neq 0$.

Proof. Res $(g,\ f) \in k[y_1, \ldots, y_d]$ is non-zero, as g is irreducible, and $g \not| f$

Proof of Algorithm. We prove the result by induction on n, it being clear for $n = 1$. let $n > 1$. Two cases arise:

• x_1 is algebraically independent modulo $\mathfrak{p}$. Let $K = k(x_1)$, and $\mathfrak{q} = \mathfrak{p} \subset K[x_2, \ldots, x_n]$. Then one verifies that G is a Gröbner base for $\mathfrak{q}$ with respect to the lexicographic order $x_2 < \cdots < x_n$. One easily checks that the variables $\{x_1,\ x_{i_1}, \ldots, x_{i_k}\}$, $i_j \neq 1$, for all j, are algebraically independent modulo $\mathfrak{p}$ in $k[x_1, \ldots, x_n]$ iff $\{x_{i_1}, \ldots, x_{i_k}\}$ are algebraically independent modulo $\mathfrak{q}$ in $K[x_2, \ldots, x_n]$.

Thus, $|T_{\mathfrak{p}}| = |T_{\mathfrak{q}}| + 1$. By induction, $\mathrm{ht}\,(\mathfrak{q}) = |T_{\mathfrak{q}}|$. But $\mathrm{ht}\,(\mathfrak{p}) = \mathrm{ht}\,(\mathfrak{q}) + 1 = |T_{\mathfrak{q}}| + 1 = |T_{\mathfrak{p}}|$, as required.

• x_1 algebraic modulo $\mathfrak{p}$. Let $g(x_1) \in k[x_1] \cap G$ be an irreducible polynomial.

Let $K = k[x_1]/(g(x_1))$, and $\mathfrak{q}$ be the image of $\mathfrak{p}$ in $K[x_2, \ldots, x_n]$. Now $T_{\mathfrak{q}}$ is algebraically dependent modulo $\mathfrak{q}$ and $|T_{\mathfrak{q}}| = \mathrm{ht}\,(\mathfrak{q})$ by induction.

Claim. $\{x_{i_1}, \ldots, x_{i_d}\}$, $i_j \neq 1$ for all j, are algebraically independent modulo $\mathfrak{q}$ in $K[x_2, \ldots, x_n]$.

This is because if there exists a non-zero polynomial $F \in \mathfrak{q} \cap k[x_{i_1}, \ldots, x_{i_d}]$, and let $f \in k[x_1,\ x_{i_1}, \ldots, x_{i_d}] \cap \mathfrak{p}$ be a lift of F. Then $f \notin (g)$. By above Lemma $\{x_{i_1}, \ldots, x_{i_d}\}$ are algebraically dependent modulo $\mathfrak{p}$ in $k[x_1, \ldots, x_n]$. The converse is obvious.

In view of the claim $ht(\mathfrak{p}) = ht(\mathfrak{q})$. Now check that G is a Gröbner base for $\mathfrak{q}$ with respect to lexicographic order $x_2 < \cdots < x_n$. Hence, $|T_\mathfrak{p}| = |T_\mathfrak{q}|$. Thus, $\mathrm{ht}\,(\mathfrak{p}) = |T_\mathfrak{p}|$, as required to be shown.

Remark. If I is non-prime then height (I) may not equal $|T_I|$. For example, take $I = (x^2,\ xy) \subseteq k[x,y]$, with $x < y$. For a correct definition of T_I refer to the paper of Kredel-Weispfenning.

Computational Noether Normalization Lemma

We present A. Logar's computational proof of the Noether normalization. The advantage of his method is that is generally requires computation of only two Gröbner bases. (The standard proof would need computation of Gröbner base of an ideal I with respect to new variables to be done height I times.)

The Noether normalisation Lemma states that an ideal I in a polynomial ring $k[x_1, \ldots, x_n]$ can be transformed by a suitable linear change of co-ordinates,

$$\begin{aligned} L : k[x_1, \ldots, x_n] &\rightarrow k[x_1, \ldots, x_n], \\ L(x_i) &= \sum_{j=1}^{n} a_{ij}\ x_j, \end{aligned}$$

$a_{ij} \in k$, provided the base field k is infinite, so that if $y_i = L(x_i)$ then $y_1, \ldots, y_d$ are algebraically independent modulo I, and $y_{d+1}, \ldots, y_n$ are integral over $k(y_1, \ldots, y_d)$ modulo I.

We say L puts I into *Noether normal position.* The usual proof also shows that the set of choices $(a_{ij}) \in k^n$ is a dense open set in the Zariski topology on k^n. Hence, the best way, one would think, is to take an arbitrary choice of (a_{ij}) and check that it works!

We now sketch A. Logar's simplified approach to put a prime ideal $\mathfrak{p}$ in Noether normal position. We fix a lexicographic ordering $x_1 < \cdots < x_n$, and a reduced Gröbner base G of $\mathfrak{p}$.

Definition. x_s is said to be *integral over* $k[x_1, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$ if there exists a non-zero polynomial $f \in \mathfrak{p} \cap k[x_1, \ldots, x_{s-1}]$ which is monic in x_s.

Lemma. x_s is integral over $k[x_1, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$ iff there is a polynomial $f \in G$ with $L(f) = x_s^m$, for some m.

Proof: If x_s integral and $f \in \mathfrak{p} \cap k[x_1, \ldots, x_{s-1}]$ monic in x_s then $L(f) = x_s^k \in (G)$. Hence $L(g) \mid x_s^k$, for some $g \in G$, whence $L(g) = x_s^m$, for some m.

Lemma. If x_s is integral over $k[x_1, \ldots, x_{s-1}, x_{i_j}, x_{i_{j+1}}, \ldots, x_{i_s}]$ modulo $\mathfrak{p}$ then x_s is integral over $k[x_1, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$. (Here $x_{i_j}, \ldots, x_{i_g}$ denote the indeterminates in $T_\mathfrak{p}$ which are greater than x_s.)

Proof: $0 \neq f \in k[x_1, \ldots, x_{s-1}, x_s, x_{i_j}, \ldots, x_{i_g}] \cap \mathfrak{p}$. If $f = x_s^m + h(x_1, \ldots, x_s, x_{i_j}, \ldots, x_{i_\delta}) \in \mathfrak{p}$, with $\mathrm{degree}_{x_s}(h) < m$.

If $L(f) \in k[x_1, \ldots, x_s]$ then $f \in k[x_1, \ldots, x_s], L(f) = x_s^m$, and x_s is integral over $k[x_1, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$.

If $L(f) = gh$, $g \in k[x_1, \ldots, x_s]$, $h \in k[x_{i_j}, \ldots, x_{i_\delta}]$, $h \neq 1, = g, h$ monomials, then $\text{degree}_{x_s} g < m$, and $f \notin G$ by the construction of $T_{\mathfrak{p}}$. The construction shows that

$$G \cap k[x_1, \ldots, x_s,\ x_{i_j}, \ldots, x_s] = k[x_1, \ldots, x_s].$$

Choose $p \in G$ such that $L(p) \mid L(f)$. Then $p \in k[x_1, \ldots, x_s]$. Moreover, let $f \to f_1$ after reducing modulo p. If $f_1 = x_s^m + h_1(x_1, \ldots, x_s,\ x_{i_j}, \ldots, x_{i_\delta})$, with $L(f_1) = x_s^m$, then we are in earlier case. If not, continue above procedure till we are reduced to that case !

We now state A. Logar's probabilitic algorithm which puts the ideal $\mathfrak{p}$ in Noether normal position. Some explanation why it will work is then given.

Noether normal position (A. Logar)

Algorithm:

Input:	A prime ideal $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$.
Output:	a $n \times n$ matrix A such that $\mathfrak{p}$ is in Noether position with respect to the variables $X := AX$.
Step 1:	Compute a Gröbner base G of $\mathfrak{p}$ with respect to the lexicographic order $x_1 < x_2 < \cdots < x_n$. Also compute $T_{\mathfrak{p}}$. Set $A = I_n$;
Step 2:	Rename the variables : Call $x_1, \ldots, x_s$ the elements of $T_{\mathfrak{p}}$, and $x_{d+1}, \ldots, x_n$ the rest of the variables. Set on $k[x_1, \ldots, x_n]$ the (new) lex order $x_1 < \cdots < x_n$ and call A_1 the permutation matrix which gives this transformation. Set $A := A_1 A_0$.
Step 3:	Compute $J = \{s \mid x_s \text{ is integral over } k[x_1, \ldots, x_{s-1}] \text{ modulo } \mathfrak{p}\}$;
Step 4:	For $r = 1$ to d let $a_{rr} := 1$, $a_{ir} := 0$ if $i \neq r$; for $r = d+1$ to n if $r \in J$ then let $a_{rr} := 1,\ a_{ir} = 0$ if $i \neq r$ else choose $a_{1r}, \ldots, a_{dr} \in k$ randomly, $x_i := x_i + a_{ir} x_r,\ i = 1, \ldots, d$; let $a_{rr} := l$; $a_{ir} := 0$ if $i \neq 1$, $i > r$; $A_2 := (a_{ij})$; $A := A_2 A$
Step 5 :	Compute a Gröbner base G of $\mathfrak{p}$ with respect to the lex order $x_1 < \cdots < x_n$.
Step 6 :	if $(G \cap k[x_1, \ldots, x_s]) \neq 0$ or (there exists $s = d+1 \leq s \leq n$ such that a power of x_s does not appear as a leading monomial of an element of G); then go to step 2.

At the end of this algorithm one has $\mathfrak{p}$ in Noether normal position with respect to the new variables $X := AX$.

Brief Explanation. The usual argument shows that for almost every λ_i (i.e. for all λ_i which are not a zero of a suitable polynomial), one has that new variables $x_i' = x_i + \lambda_i\, x_r$, if $i \leq d$, $x_i' = x_i$, if $i > d$, are algebraically independent modulo $\mathfrak{p}$ and $x_r' = x_r$ is integral over $k[x_{i_j}', \ldots x_s']$. This is because $\mathfrak{q} = \mathfrak{p} \cap k[x_1, \ldots, x_s]$ is a non-zero prime ideal of height one, whence a principal ideal, say $\mathfrak{q} = (f)$. If $f(-\lambda_0, \ldots, -\lambda_d, 1) \neq 0$, then x_r is seen to be integral over $k[x_1', \ldots, x_d']$ modulo $\mathfrak{q}$, and hence modulo $\mathfrak{p}$.

Note that $x_s' (= x_s)$ is integral over $k[x_1', \ldots, x_d', x_{d+1}]$ modulo $\mathfrak{p}$ for $s < d$, $s \neq r_j$ and that if $r < s$, and x_s is algebraic but not integral over $k[x_1, \ldots, x_d,\ x_{d+1}, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$ then $x_s' = x_0$ is algebraic but not integral over $k[x_1, \ldots, x_d,\ x_{d+1}, \ldots, x_{s-}]$.

Consider the transformation

$$A : x_i' = x_i + \sum a_{is} x_s,\ i = 1, \ldots, d$$

$s \notin J,\ s > d$. For almost all choices of $a_{i_j},\ 1 \le i \le d,\ j \in J,\ j > d$ one observes that $x'_1, \ldots, x'_d$ are algebraically independent modulo $\mathfrak{p}$, and that x_{d+i} is integral over $k[x'_1, \ldots, x'_s]$ modulo $\mathfrak{p}$ for $i = 1, \ldots, n-d$:

This is because if $r = \min\{s \in \mathbb{N} \mid s \notin J\}$ and $u_i = x_i + a_{ir}\, x_r,\ i = 1, \ldots, d$, then

1. if $s \notin J$, and $s \neq r$, then x_s is algebraic but not integral over $k[u_1, \ldots, u_d, u_{d+1}, \ldots, x_{s-1}]$ modulo $\mathfrak{p}$.
2. If $s \in J$ then x_s is integral over $k[u_1, \ldots, u_d,\ x_{d+1}, \ldots, x_{s+1}]$ modulo $\mathfrak{p}$.
3. If $s = r$ then x_s is integral over $k[u_1, \ldots, u_d]$ modulo $\mathfrak{p}$.

Hence, $s > d$, x_s is integral over $k[u_1, \ldots, u_d, x_{d+1}, \ldots, x_{s-1}]$ modulo $\mathfrak{p} = J \cup \{r\}$. Repeat the procedure to get the result.

2 Orderings, Elimination, Computing Radicals

Examples of monomial orderings.

(1) **Lexicographic order:** $<_{lex}$: $x_1 <_{lex} x_2 <_{lex} \cdots <_{lex} x_n \equiv$

$$\begin{array}{rcl} x_1^{a_1} \cdots x_n^{a_n} & < & x_1^{b_1} \cdots x_n^{b_n} \\ & & \text{if} \quad a_1 = b_1, \cdots, a_{r-1} = b_{r-1}, a_r < b_r, \\ \equiv \alpha = (a_1, \cdots, a_n) & < & (b_1, \cdots, b_n) = \beta \end{array}$$

if first non-zero entry of $\beta - \alpha$ is positive.

(2) **Product ordering.** Combine several admissible partial orders by "lexicographic product" of orderings:

$$\begin{array}{rcl} T & = & T_1 \times_{lex} T_2 \times_{lex} \cdots \times_{lex} T_r \\ m_1 & = & x_1^{a_1} \cdots x_n^{a_n} \ <_T \ x_1^{b_1} \cdots x_n^{b_n} = m_2 \text{ iff} \\ m_1 & =_{T_1} & m_2, \cdots, m_1 =_{T_{i-1}} m_2, \quad m_1 <_{T_i} m_2 \\ & & \text{for some } 1 \le i \le n \end{array}$$

(3) **Degree or graded orders.** A graded monomial order is one that orders first by total degree. In general, a degree order is got by taking a product of total degree partial order and another partial order, say *lex*. For example, we have: $glex$ = graded lexicographic order:

$$\alpha = (\alpha, \cdots, \alpha_n) \quad < \quad (b_1, \cdots, b_n) = \beta$$

if the first non-zero entry of

$$(\sum \beta_i - \sum \alpha_i, b_1 - a_1, \cdots, b_n - a_n)$$

is positive.

(4) **Graded reverse lexicographic order.** *Grevlex*:

$(a_1, \cdots, a_n) < (b_1, \cdots, b_n) \Leftrightarrow$ last non-zero entry of $(\sum b_i - \sum a_i, b_1 - a_1, \cdots, b_n - a_n)$ is negative.

This is the *default monomial ordering* used in *Macaulay*[1]. This is because the amount of computation needed to produce a Gröbner bases is minimized by using this term ordering. Also, Bayer-Stillman have shown that the total degrees of bases elements obtained is smaller in most cases.

In practice, one therefore computes using *grevlex*. One then applies algorithms which convert a Gröbner bases with respect to one ordering to a Gröbner bases with respect to another ordering, for example

1. **FGLM algorithm:** due to Faugers-Giani-Lazard-Mora.
2. **Traverso's method:** He uses Hilbert functions.
3. **Gröbner walk:** by Collart, Kalkbremer, Mall.
4. **Fractal walk:** by Trân

(First two are for codim zero ideals. 2^{nd} is implemented in Singular.[2] The last two are for general ideals.)

Let us summarize the characteristic properties of *lex, glex, grevlex*:

1. Let $f \in R$ with $L_{lex}(f) \in k[x_s, \cdots, x_n]$, for some $1 \leq s \leq n$. Then $f \in k[x_s, \cdots, x_n]$.
2. Let $f \in R$ with $L_{glex}(f) \in k[x_s, \cdots, x_n]$, for some $1 \leq s \leq n$. If f is homogeneous, then $f \in k[x_s, \cdots, x_n]$.
3. Let $f \in R$ with $L_{lex}(f) \in k[x_s, \cdots, x_n]$, for some $1 \leq s \leq n$. If f is homogeneous, then $f \in (x_s, \cdots, x_n)$.

We leave it to the reader to check these details. (See Elimination theorem below for comparison.)

(5) **Elimination orders on** $\{x_1, \cdots, x_n, y_1, \cdots, y_m\}$. Let $<_x, <_y$ be term orders on $\{x_i\}, \{y_i\}$ respectively. The lexicographic product order $<=<_x \times <_y$: $x^\alpha y^\beta < x^{\alpha'} y^{\beta'}$ if $x^\alpha <_x x^{\alpha'}$ or $x^\alpha = x^{\alpha'}, y^\beta <_y y^{\beta'}$ is s.t.b an Elimination order with x variables larger than the y variables. Elimination orders derive their name from the following important property:

Elimination Theorem. Let I be an ideal of $k[x_1, \cdots, x_n, y_1, \cdots, y_m]$ and $<$ be an elimination order with x variables larger than y variables. Let $G = \{g_1, \cdots, g_t\}$ be a Gröbner bases for I. Then $G \cap k[y_1, \cdots, y_m]$ is a Gröbner bases for $I \cap k[y_1, \cdots, y_m]$.

Proof: Let $0 \neq f \in I \cap k[y_1, \cdots, y_m]$. $L(f) \in L(I) =< L(g_1), \cdots, L(g_t) >$. Let $L(g_{i_1}) \mid L(f)$ for some i_0. Hence, $L(g_{i_0}) \leq L(f)$. Note that $L(g_{i_0})$ will only have y variables. Now no monomial of g_{i_0} can have any x-variables as a monomial having x variables $> L(f)$!. Hence $g_{i_0} \in k[y_1, \cdots, y_m]$. Hence, $\forall f \in I \cap k[y_1, \cdots, y_m]$ $\exists$ $g_i \in$

[1] available via anonymous ftp at zariski.harvard.edu

[2] See the Singular homepage at http://www.mathematik.uni-kl.de/~̃ca/Singular/

$G \cap k[y_1, \cdots, y_m]$ such that $L(g_i) \mid L(f)$, whence $G \cap k[y_1, \cdots, y_m]$ is a Gröbner bases for $I \cap k[y_1, \cdots, y_m]$.

□

Normal form

The monomials M which do not lie in $L(I)$ are called *standard monomials*; otherwise M is called a *non-standard monomial.*

Definition. For a given $f \in k[x_1, \cdots, x_n]$ the unique polynomial

$$NF(f) = \sum_{\alpha} c_\alpha x^\alpha, c_\alpha \in k,$$

where each x^α is a standard monomial, and such that $f - NF(f) \in I$ called the *normal form* of f with regard to the chosen order.

Existence: Let $f \in R$. Let $m = hnst(f)$ be the highest non-standard monomial in f. Then $m \in < Lg_1), \cdots, L(g_r) >$ implies $m = L(g_{i_0})m'$, for some i_0. Let $f_1 = f - m' g_{i_0}$, then $hnst(f_1) < hnst(f)$. Hence this algorithm will terminate, and eventually only standard monomials will occur.

Theorem (Macaulay) (Normal Form) Let R be the polynomial ring in n variables over a field, and I be an ideal of R. Then the set of residue class of standard monomials is a basis for the vector space R/I, i.e.

Normal form $NF : R/I \to R/L(I)$,

is an isomorphism of vector spaces over k.

Proof. We have just seen that NF is surjective. NF is injective: Let $f \in R$ with $NF(f) \in L(I)$. Clearly, every term of $NF(F)$ is in $L(I)$, whence is non-standard!. This can only happen if $NF(f) = 0$, i.e. $f \in I$.

Remark. There are algorithms to calculate NF and one such is the Buchberger algorithm. There are others which calculate Normal Form with respect to an ordering which need not even be a well-order! These are the *tangent cone orderings*, and the algorithm is due to Mora. Since the order is not a well-order these are called standard rather than Gröbner bases. Such orders are needed, say, when studying questions about singular points.

Computation of Ideals via Gröbner bases

We will now spend some time in calculating various ideals: saturation of an ideal with respect to another ideal, homogenization and dehomogenization of ideals, radical membership.

Elimination and intersection of ideals.

Let t be a new variable then

$$I \cap J \quad = \quad (It + J(1-t)) \cap R.$$

If $a \in I \cap J$, then $a = at + (1-t)a$. Conversely, let $a = \sum a_i h_i(t) t + \sum b_j g_j(f)(1-t)$, with $a_i \in I,\ b_j \in J,\ h_i(t),\ g_j(t) \in R[t]$. Evaluate at $t = 0,\ 1$, to get $a \in I \cap J$. Hence, compute $I \cap J$ as follows: Let G be a Gröbner base for $It, J(1-t))$ w.r.t. an elimination order with $x_i < t$, for all i. By Elimination theorem, $G \cap k[x_1, \ldots, x_n]$ is a Gröbner base for $I \cap J$.

Quotient ideals and Gröbner bases

Given two ideals $I,\ J$ of R their *quotient ideal* $I : J$ is the ideal $\{r \in R \mid rJ \subseteq I\}$.

If $J = (a_1, \ldots, a_n)$ then it is easy to see that $(I : J) = \bigcap_{i=1}^{n}(I : (a_i))$. Moreover, for each i,
$(I : (a_i)) = \frac{1}{a_i}(I \cap (a_i))$. Since $I \cap (a_i)$ can be computed using an *elimination order*, so can each $(J : (a_i))$, whence we can compute $(I : J)$.

Alternative Method: Let $f(t) = a_1 + a_2 t + \cdots + a_n t^{n-1}$, then $(I : (a_1, \ldots, a_n)) = (IR[t] : (f(t))) \cap R$. The equality is easy to see. This method reduces the calculation to a single computation.

Remark. Ideal quotients can be used to compare two ideal for containment: If $I \subset J$, then $(I : J) = 1$ iff $I = J$.

Saturation of an ideal I w.r.t. ideal J.

More generally, one has

$$(I : J^\infty) = \bigcup_{n \geq 0}(I : J^n),$$

the *saturation of* I with respect to J. This operation will strip away from any primary decomposition of I all the components whose radical contians J. (Check this!) Bayer-Stillman give the following device to compute it:

Let $J = (a_1, \ldots, a_n)$, $f = a_1 + a_2 + \cdots + a_n t^{n-1}$. Then $(I : J^\infty) = ((I,\ y - f) : y^\infty) \cap R$.

Graded Reverse lexicographic order and the saturation of an ideal

The chain of ideals

$$(I : f) \subseteq (I : f) \subseteq (I : f^2) \subseteq \cdots$$

is stationary at $(I : f^n) = (I : f^{n+1}) = \cdots$. This limit is denoted by

$$(I : f^\infty) = \{g \in R \mid gf^m \in I \ \text{ for some } m\}$$

and is called the *saturation* of I with respect to f. This construction is useful when we try to compute primary decomposition of an ideal. For instance, it permits us to concentrate on certain primary components and to leave out the rest : Let $I \subseteq (x_0, \ldots, x_n)$ be a homogeneous ideal. Then $(I : x_n^\infty)$ is "saturated" because it cannot have $(x_0, \ldots, x_n)$ as an associated prime: If $I = \bigcap_{i=1}^{r} \mathfrak{q}_i$, then $(I : x_n^\infty) = (\bigcap_{i=1}^{r} \mathfrak{q}_i : x_n^\infty) = \bigcap_{i=1}^{r}(q_i : x_n^\infty)$. Now $(q_i : x_n^\infty) = \mathfrak{q}_i$ if $x_n \notin \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, and $(\mathfrak{q}_i : x_n^\infty) = R$ if $x_n \in \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Hence, $(I : x_n^\infty) = \bigcap_{x_n \notin \mathfrak{p}_i} \mathfrak{q}_i$, and where $x_n \in \mathfrak{p}_j$'s for all other $\mathfrak{p}_j$'s occuring.

Lemma. If $\{x_n^{a-1} g_1, \ldots, x_n^{a_r} g_r\}$ is a Gröbner base for I with respect to *grevlex*, and $x_n \not| g_1$, for all i, then $G = \{g_1, \ldots, g_r\}$ is a Gröbner base for $(I : x_n^\infty)$.

Proof. Clearly, $G \subset (I : x_n^\infty)$. Let $f \in (I : x_n^\infty)$, and let $x_n^\infty f \in I$. Then $L(x_n^m f)$ is divisible by $L(x_n^{q_{i_0}} f_{i_0})$ for some i_0. Since $x_n \not| f_{i_o}$, hence $L(f_{i_0}) \mid L(f)$!

Graded monomial orders and the homogenization of an ideal.

Given $0 \neq f \in R = k[x_1, \dots, x_n]$, the *homogenisation* of f is the polynomial

$$^h f = x_0^{\deg(f)} f(\frac{x_1}{x_0}, \cdots, \frac{x^n}{x_0}).$$

Thus, if $f = f_d + f_{d-1} + \cdots + f_0$, with f_i homogeneous of degree i, then
$$^h f = f_d + x_0 f_{d-1} + \cdots + x_0^d f_0 \in k[x_0, \dots, x_n].$$

Given a homogeneous polynomial $F \in S$ of degree d, we define its *dehomogenization* $^a F \in R$

$$^a F = F(1, x_1, \dots, x_n) \in R$$

If I is an ideal of R, then

$$^h I = \{^h f \mid f \in I,\ f \neq 0\}$$

is called the *homogenization* of I. The reader should check that $^h I$ is a homogeneous ideal! Note that if $I = (f_1, \dots, f_r)$ then $^h I$ need not be the ideal $(^h f_i, \dots, ^h f_r)$. For example, let $I = (x_2 - x_1^2, x_3 - x_1^3)$, then $f_3 = x_3 - x_1 x_2 = f_2 - x f_1 \in I$. It can be easily verified that $f_3^h \notin (f_1^h,\ f_2^h)$.

However, if $f_1, \dots, f_r$ is a Gröbner base of I *then* $(^h f_1, \dots, ^h f_r)$ *is a Gröbner base of* $^h I$ with respect to a suitable order which extends the order $>$ on R, viz. define $x^\alpha x_0^d >_h x^R x_0^e$ iff $x^\alpha > x^\beta$ or $x^\alpha = x^\beta$ and $d > e$.

To see this first observe that

Lemma $L_{>_h}(^h f) = L_>(f)$

Proof. The monomial of total degree of F appear unchanged in $^h f$, whereas all other monomials are divisible by x_0. Hence, $L_>(f) = x_1^{\alpha_1} \dots x_n^{\alpha_n} >_n L(x_0^e x_1^{\beta_1} \dots x_n^{\beta_n})$ if $e \geq 1$ and if $x_1^{\beta_1} \dots x_n^{\beta_n}$ is a monomial of f. Clearly, it follows that $L_{>_h}(f) = x_1^{\alpha_1} \dots x_n^{\alpha_n} = L_>(f)$.

It sufficies to show that

$$L_{>_h}(^h I) = (L_{>_h}(^h f_1) \dots, L_{>_h}(^h f_r)).$$

Since $^h I$ is homogeneous, for any $F \in {}^h I$, each homogeneous component of F is in $^h I$. So we assume $F \in {}^h I$ is homogeneous and show $L_{>_h}(F)$ is in the right hand side ideal. Let $F = \sum a_j\ ^h g_j$, for some $g_j \in I,\ a_j \in S$. The $f =^a F = \sum^a a_j\ ^a(^h g_j) = \sum^a a_j g_j$, and so $f \in I$. Now, $F = x_0^e(^h f)$, for some $e \geq 0$. Hence, $L_{>_n}(F) = x_0^e L_{>_n}(^h f) = x_0^e L_>(f)$. Since $\{f_1, \dots, f_r\}$ is a Gröbner base of I, $L_>(f_{i_0}) \mid L(f)$, for some i_0. But $L_>(f_{i_0}) = L_{>_h}(^h f_{i_0})$. Hence $L_{>_h}(^h f_{i_0})$ divides $L_{>_h}(F)$, for some i_0.

Corollary. Let $G = \{g_1, \dots, g_r\}$ be a Gröbner base of an ideal with respect to the *grevlex* order on $R = k[x_1, \dots, x_n]$. Then $^h G$ is a Gröbner base for $^h I \subset S = k[x_1, \dots, x_{n+1}]$ with respect to the *grevlex* order.

Finally we remark that if $\{f_1, \dots, f_r\}$ is a homogeneous base of $^h I$ then $\{^a f_1, \dots, ^a f_r\}$ is a Gröbner base for I.

Proof. Let $f \in I$, then $^h f = \sum h_i f_i$, for some homogeneous $h_i \in S$. Hence, $f =^a (^h f) = \sum^a h_i^a f_i$, and $\deg(^a h_i^a f_i) \leq \deg(h_i f_i) = \deg(^h f) = \deg f$. Hence,

$$L(f) = \sum L(^a h_i) L(^a f_i) \in (L(^a f_1), \dots, L(^a f_r))$$

as was required to be shown.

Exercise. If $I = (f_1, \dots, f_m)$ then show that ${}^hI = (({}^hf_1, \dots, {}^hf_m) : x_0^\infty)$. (This shows that the right hand side ideal is independent of the set of generators of I chosen.)

Exercise. $(\sqrt{{}^hI})_{x_0=1} = \sqrt{I}$

Radical Membership.

Let t be a new variable. Then $f \in \sqrt{I}$ iff $(I, 1 - tf) = R[t]$. (This is easily checked).

Hence if we compute the reduced Gröbner base of $(I, 1 - tf)$ we can decide whether $f \in \sqrt{I}$ depending on whether this is $\{1\}$ or not.

To actually compute $\sqrt{I}$ is known in several cases, especially when I is an *unmixed* ideal, i.e. when all the primary components of I have the same codimension. These computations generalise, to several variables, the venerable formula,

$$\begin{aligned}\sqrt{(f)} &= (f) :_{k[t]} df/dt \\ &= (f) : f' \\ &= (f(x)/g.c.d.(f(x), f'(x)))\end{aligned}$$

More details of these methods can be found in the book of W. Vasconcelos. These ideas have been illustrated in the Macaulay II practical sessions on the web.

The Extension Theorem

The Elimination theorem is useful in solving equations via the Extension theorem, which enables one to recursively, by induction on the number of of variables, find solutions. The situation is as follows : Given $f_1(x_1), \dots, f_s(x_1) \in k[x_2, \dots, x_n][x_1]$, find a common solution.

Method: Choose an elimination order $<$ with $x_1 > x_2 > \cdots > x_n$. Let G_1 be a Gröbner base for $I = (f_1,(x_1), \dots, f_s(x_1))$ with respect to $<$, and let $I_1 = I \cap k[x_2, \dots, x_n]$. Then by the Elimination theorem, $G \cap k[x_2, \dots, x_n]$ is Gröbner base for I. Assume inductively we can find a common solution of $V(I_1)$: let

$(a_2, \dots, a_n)$ be a common root of $V(I_1)$. *Assume further that* $(a_2, \dots, a_n)$ is *not* a common solution of $L(f_1(x_1)), \dots, L(f_s(x_1))$.

In this set up, we have

Extension Theorem: If k is algebraically closed, then there is $a_1 \in k$ such that $(a_1,\ a_2, \dots, a_n)$ is a common solution of $f_1 = 0,\ f_2 = 0, \dots, f_s = 0$

By reducing to the univariate case

We sketch a method to algorithmically find the fintely many zeros of a zero-dimensional ideal. The method is by "trial and error", but has Elimination technique and the Extension Theorem rooted in its background.

Let I be an ideal of $R = k[x_1, \dots, x_n]$ generated by a subset F. Construct a Gröbner base G for I with respect to lexicographic order $x_1 < x_2 < \cdots < x_n$. By Elimination, $G_k = G \cap k[x_k, \dots, x_n]$ is a Gröbner base for $I \cap k[x_k, \dots, x_n]$.

Find the g.c.d. P_n of the univariate polynomials in $G_n = G \cap k[x_n]$. Find a zero $\zeta_n \in \overline{k}$ of P_n. If P_n has no zero then $V(I) = \emptyset$.

Suppose that $\zeta_{k+1}\ldots,\zeta_n \in \overline{k}$ have already been found. Let $G_k(\zeta_{k+1}\ldots,\zeta_n)$ be the univariate polynomials in x_k obtained from G_k by substituting ζ_j for $x_j, for\ k+1 \leq j \leq n.$

Compute the g.c.d. P_k of the polynomials in $G_k(\zeta_{k+1},\ldots,\zeta_n)$. Find a zero $\zeta_k \in \overline{k}$ of P_k. If P_k has no zero in $\overline{k}$, we have to go back to G_n, and to find another sequence $\zeta_n,\ldots,\zeta_{k+1}$.

If we obtain $(\zeta_1,\ldots,\zeta_n)$ by this algorithm, it is an element of $V(I)$.

Note that by the Elimination Theorem all the zeros of I can be computed in this way: For if $(\zeta_1,\ldots,\zeta_n)$ is a common zero than $P_n(\zeta_n) = 0$, as $P_n \in I$. Also $P_{n-1} = g.\ c.\ d.\ \ G_{n-1}(\zeta_n)$. Since $G_{n-1} = G \cap K[x_{n-1}, x_n]$, we have $G_{n-1}(\zeta_n) = G(\zeta_n) \cap k[x_{n-1}]$. But by Elimination Theorem, $I \cap k[x_{n-1}, x_n]$ is generated by G_{n-1}. Hence, $P_{n-1}(x_{n-1}) = g.\ c.\ d.\ G_{n-1}(\zeta_n) \in < G_{n-1}(\zeta_n) >$. Since $g(\zeta_{n-1},\zeta_n) = 0$ for all $g(x_{n-1},x_n) \in G_{n-1}$, it follows that $P_{n-1}(x_{n-1}) = 0$. The general case is similar.

Radicals via Elimination

We will give another method due to Krick-Logar of computing the radical via elimination.

The actual computation of the radical of an ideal will play a crucial role in computing the associated primes of a given polynomial ideal.

We begin with the higher dimensional analog of the methods used earlier to find the radicals of zero-dimensional ideals. This method relies on rounds of eliminations. The first step is to place the ideal in a '*general position*' special in these contexts.

Placing an ideal into *Noether normal position.* The Noether noramlization lemma states that an ideal $I < R = k[x_1,\cdots,x_n]$ can be transformed by a linear change of co-ordinates:

$$\begin{aligned} L : k[x_1,\cdots,x_n] &\rightarrow k[x_1,\cdots,x_n], \\ L(x_i) &= \sum_{j=1}^{n} a_{ij}x_j, a_{ij} \in k, \end{aligned}$$

so that

$$k[L(x_1),\cdots,L(x_d)] \hookrightarrow R/I,$$

is an integral extension, and $L(x_1),\cdots,L(x_d)$ are algebraically independent. Here $d = dim(R/I)$. We say L puts I in Noether normal position. The clasical proofs show that, provided k is an infinite field, "almost all" linear changes of variables put I in normal position. A. Logar has suggested a method, when I is a prime ideal, which needs at most two Gröbner base computations. We did this algorithm earlier. If I is in normal position, then we can choose f_i to be monic in x_{d+i} with coefficients in $k[x_1,\cdots,x_d]$.

Let I be an ideal of $R = k[x_1,\cdots,x_n]$ of height m. Let $d = n - m$ be the codimension of I. (It will also be the dimension of R/I).

By Noether normalisation, after a suitable relabelling, the subring $S = k[x_1,\cdots,x_d]$ satisfies $I \cap S = (0)$, and $I \cap S[x_{d+i}] \neq 0$, for all $i > 0$. Let $0 \neq f_i \in I \cap S[x_{d+i}]$, for $1 \leq i \leq m$. Write $f_i = g_ih_i$, where g_i is the g.c.d. of the coefficients of $f_i(x_{d+1})$. Let b_i denote the square free part of h_i. Then, $p_i = g_ib_i \in \sqrt{I}$.

One can obtain f_i's by choosing an Elimination order, say with $x_1 < \cdots < x_d < x_{d+1} < \cdots < x_n$ for if G is a Gröbner base of I, then $G \cap S[x_{d+i}]$ will be a Gröbner base by Elimination Theorem, of $I \cap S[x_{d+i}]$ and so has elements f_i of desired type.

However, in the sequel besides placing the ideal in normal position, we shall also need:

(*) *If G is a Gröbner base of I then $G^e (= G)$ is a Gröbner base of $I^e = IK[x_{d+1}, \cdots, x_n]$, where $K = k(x_1, \cdots, x_d)$, with respect to the term order induced by the order amongst $x_{d+1}, \cdots, x_n$.*

To ensure (*) holds select a term order $<_1$ on $k[x_1, \cdots, x_d]$, a term order $<_2$ on $k[x_{d+1}, \cdots, x_n]$, and let $<$ be the product term order on $k[x_1, \cdots, x_n]$:
i.e. if ϕ_1, ψ_1 are terms in $k[x_1, \cdots, x_d]$, and $\phi_2, \psi_2 \in k[x_{d+1}, \cdots, x_n]$ are terms, then $\phi_1\phi_2 < \psi_1\psi_2$ iff $\phi_2 <_2 \psi_2$ or $\phi_2 = \psi_2$ and $\phi_1 <_1 \psi_1$.

With such a term order (*) holds. (Check this).

Let $q = l.c.m.L_{<_2}(g)$. (Here $<_2$ is the induced term order on $K[x_{d+1}, \cdots, x_n]$.)

We now fix a primary decomposition of $\sqrt{I}$:

$$\begin{aligned} \sqrt{I} \;=\; & (\mathfrak{p}_{m1} \cap \cdots \cap \mathfrak{p}_{1\alpha_1}) \cap (\mathfrak{p}_{m+11} \cap \cdots \cap \mathfrak{p}_{m+1\alpha_{m+1}}) \\ & \cap \cdots \cap (\mathfrak{p}_{n1} \cap \cdots \cap \mathfrak{p}_{n\alpha_n}). \end{aligned}$$

Here, $\mathbf{g}_{ij}$ is a prime ideal of height i, for all $i \geq m$, and for $1 \leq j \leq \alpha_i$. We assume further that the above decomposition is *minimal*; i.e. $\mathfrak{p}_{ij} \not\subset \mathfrak{p}_{rs}$ if $i \neq r, j \neq s$. Let for $0 \leq i \leq d$

$$I_{m+i} = \bigcap_{1 \leq j \leq \alpha_{m+i}} \mathfrak{p}_{m+ij}.$$

Then I_{m+i} is an equidimensional radical ideal of height $m+i$, and

$$\sqrt{I} = I_m \cap I_{m+1} \cap \cdots \cap I_n.$$

Note that if I is in normal position then

$$k[x_1, \cdots, x_d] \cap \mathfrak{p}_{mj} = 0,$$

for all $1 \leq j \leq \alpha_m$.

Proof. If the intersection is non-zero, for some j, then the proof of Noether normalization shows that we have a Noether subring

$$k[x_{i_1}, \cdots, x_{i_r}] \hookrightarrow R/\mathfrak{p}_{mj},$$

with $\{i_1, \cdots, i_r\}$a proper subset of $\{1, \cdots, d\}$. This means $dim R/\mathfrak{p}_{mj} < d$, a contradiction.

This information is special to I_m and we will exploit it to describe I_m explicitly. The main result is

Theorem (Krick-Logar)
(i) The ideal I_m equals the saturation ideal $((I, p_1, \cdots, p_m) : q^\infty)$.
(ii) $\sqrt{I} = I_m \cap \sqrt{(I, p_1, \cdots, p_m, q)}$.

Remark. The theorem gives us an explicit algorithm to compute $\sqrt{I}$. For by placing I in normal position, and choice of term order $<$, we can get $f_1, \cdots, f_m, g_1, \cdots, g_m, h_1, \cdots, h_m$. The square roots $b_1, \cdots, b_m$ can be computed, in characteristic zero, via.,

$$b_i = h_i / g.c.d.(h_i, \partial h_i / \partial x_{d+i}),$$

for $1 \leq i \leq m$. (In positive characteristics $p > 0$, one needs to assume the field is perfect and to be able to extract the p-th root.) We can now use the algorithm to compute saturation, and get I_m.

Note that $(I, p_1, \cdots, p_m, q)$ has codimension $\geq m+1$, as its intersection with $S[x_{d+i}]$ is non-zero, for $1 \leq i \leq m$.

Thus, we can can start with it, and find its $(m+1)$-th equi-dimensional component, etc. Finally, we express $\sqrt{I}$ as an intersection of computable radical equidimensional ideals. Using algorithms for intersection of ideals gives $\sqrt{I}$.

Remark. The above method shows how the equidimensional component I_m of an ideal I of codimension m can be computed. Later we shall see how the other components I_k, $k \geq m$, can also be explicitly computed. The idea of this comes from the following description of I_m.

Proposition (Computation of I_m via 1regular sequences)

Let I be an ideal of codimension m. Let $x = x_1, \cdots, x_m$ be a regular sequence in I. Then

$$I_m = (x) : ((x) : I) \simeq Ext^m_R(R/I, R).$$

The last equality is a consequence of a famous lemms of Rees.

Proof of Theorem. Let $J = (I, p_1, \cdots, p_m)$. We shall show that

$$(J : q^\infty) = J^{ec} = I_m^{ec} = I_m$$

if J is in normal position. Here the extension and contraction are with respect to the inclusion of rings

$$k[x_1, \cdots, x_n] \hookrightarrow k(x_1, \cdots, x_d)[x_{d+1}, \cdots, x_n].$$

Step 1. $J^{ec} = J_m^{ec} = I_m$. Note that

$$I_j \cap k[x_1, \cdots, x_d] = \begin{cases} 0 \text{ if } j = m \\ \neq 0 \text{ if } j > m \end{cases}$$

Hence, $(\sqrt{I})^{ec} = (I_m \cap \cdots \cap I_n)^{ec} = I_m^{ec} \cap \cdots \cap I_n^{ec} = I_m^{ec} = (\cap_j \mathfrak{p}_{m_j})^{ec} = \cap \mathfrak{p}_{m_j}^{ec} = \cap \mathfrak{p}_{m_j} = I_m$. (Note $\mathfrak{p}_{m_j}^{ec} = \mathfrak{p}_{m_j}$ is due to the earlier observation that $\mathfrak{p}_{m_j} \cap k[x_1, \cdots, x_d] = (0)$, for $1 \leq j \leq \alpha_m$.)

Now, $I \subseteq J \subseteq \sqrt{I}$ gives $I^e \subseteq J^e \subseteq (\sqrt{I})^e$, whence $I^{ec} \subseteq (\sqrt{I})^{ec} = I_m$.

Now observe that J^{ec} is a radical ideal in view of the following Lemma.

Lemma. Let J be an ideal in $R = k[x_1, \cdots, x_n]$ such that for each i there exists a square free polynomial $\phi_i \in J \cap k[x_i]$. Then J is a zero-dimensional radical ideal.

Proof. Clearly, J is zero-dimensional. Further,

$$\frac{k[x_1, \cdots, x_n]}{(p_1, \cdots, p_n)} \simeq \frac{k[x_1]}{(p_1)} \otimes \frac{k[x_2]}{(p_2)} \otimes \cdots \otimes \frac{k[x_n]}{p_n)}.$$

Each component is a finite product of fields, as p_i is square free. Hence above ring is semi-simple, and so is its quotient ring R/J. Thus, R/J has no nilpotent elements, and J is a radical ideal.

In view of the lemma, $I^{ec} \subseteq J^{ec} \subseteq I_m$ implies, on taking radicals,

$$\sqrt{I^{ec}} \subseteq \sqrt{J^{ec}} \subseteq \sqrt{I_m}, i.e. (\sqrt{I^e})^c = I_m \subseteq J^{ec} = \sqrt{J^{ec}} \subseteq I_m = \sqrt{I_m};\text{ whence } J^{ec} = I_m.$$

Step 2. Let J be any ideal in normal position of height d, and let q be defined as above. Then $J^{ec} = (J : q^\infty)$. $f \in (J : q^\infty)$ implies $fq^r \in J$ for some r. Hence, $f \in J_q \subseteq J^e = Jk(x_1, \cdots, x_d)[x_{d+1}, \cdots, x_n]$. Thus, $(J : q^\infty)$ is a subset of J^{ec}.

Conversely, $f \in J^{ec}$ iff there exists $a \in k[x_1, \cdots, x_d]^*$ such that $af \in J$. Now we shall show that

(**) $k[x_1, \cdots, x_n]\mu/J_q$ is a free $k[x_1, \cdots, x_s]_q$-module.

But then $af \in J$ implies $f \in J_q$. Equivalently, $f \in (J : q^\infty)$. Thus, $J^{ec} \subseteq (J : q^\infty)$.

To prove (**) observe that if G is a Gröbner base of J.

1. $G^e (= G)$ is a Gröbner base of J^e with respect to $<_2$ induced on $K[x_{d+1}, \cdots, x_n]$.

2. J^e is zero-dimensional. Hence, $K[x_{d+1}, \cdots, x_n]/J^e$ is a finite dimensional vector space. To get a basis: Take all terms of $K[x_{d+1}, \cdots, x_n]$ reduced with respect to G^e. By Macaulay's theorem they form a basis. Call it B.

3. The monomials $b = x_{d+1}^{j_1} \cdots x_n^{j_{n-d}}$ generate $k[x_1, \cdots, x_n]$ as a $k[x_1, \cdots, x_d]$-module, whence they generate $K[x_1, \cdots, x_n]_q$ as a $k[x_1, \cdots, x_d]_q$-module. These monomials can be written in normal form with respect to G^e. However, note that by a careful argument, the process shows that there is N such that $q^N b$ is in the $k[x_1, \cdots, x_d]$-module generated by B. This is because we need to reduce with respect to G^e, hence only need to invert $L_{<_2}(g)$, for $g \in G$, i.e. to invert q. Hence, B generates $k[x_1, \cdots, x_n]_q$ as a $k[x_1, \cdots, x_d]_q$-module. Further, elements of B are algebraically independent over $K[x_{d+1}, \cdots, x_n]$, and so over $K[x_1, \cdots, x_n]_q$. Thus, B gives a basis of $k[x_1, \cdots, x_n]/J^e$ over $k[x_1, \cdots, x_d]_q$.

We now prove (ii) of the Theorem, viz. $\sqrt{I} = I_m \cap \sqrt{(I, p_1, \cdots, p_m, q)}$.

Case 1. If I is equidimensional in normal position then $\sqrt{I} = I_m = J_m^{ec} = J^{ec} = (J : q^\infty) = \sqrt{(J = q^\infty)}$ as the latter is a reduced ideal via. a previous lemma.

Lemma. If I is not equi-dimensional then $q \in I_{m+1} \cap \cdots \cap I_n$.

If not, let $\mathfrak{p}_1, \cdots gp_t \subset \{P_{ij} \mid i = m+1, \cdots, n, 1 \le j \le \alpha_i\}$ be the prime ideals associated to $\sqrt{I}$ which do not contain q. Now,

$$J = (I, p_m, \cdots, p_m) \subseteq \sqrt{I} = \bigcap_{j \ge m} I_j \subseteq I_m.$$

Therefore, $(J : q^\infty) \subseteq (I_m : q^\infty)$. But $(J : q^\infty) = J^{ec} = I_m^{ec} = I_m$, and

$$(\sqrt{I} : q^\infty) = (\bigcap_{j \ge m} I_j : q^\infty) = \bigcap_{j \ge m} (I_j : q^\infty) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t.$$

Hence, $(I_m : q^\infty) \subseteq I_m^{ec} = (J : q^\infty) \subset (\sqrt{I} : q^\infty) \subseteq \mathfrak{p}_1 \cap \cdots \mathfrak{p}_t \cap (I_m : q^\infty)$.

Therefore $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t \subset J_m^{ec}$. This contradicts the minimality of the primary decomposition of $\sqrt{I}$

We return to the proof of (ii): Due to the claim, $\sqrt{(I, p_1, \cdots, p_m, q)} \subseteq I_{m+1} \cap \cdots \cap I_n$, as the r.h.s. is a radical ideal, which contains q. Hence, $I \subset \sqrt{(I, p_1, \cdots, p_m, q)} \cap I_m \subseteq I_m \cap \cdots \cap I_n = \sqrt{I}$. Taking radicals, gives the result.

3 Computing the Normalisation of a Ring

When we study computational primary decomposition, we shall find it useful to know how to compute the normalization of a domain, i.e. an overdomain which is integrally closed in its total quotient ring. Of course, a localisation of a normal domain is normal. Moreover, any domain is the intersection of its localisations (at maximal ideals), It follows that 'Normality is a local property', i.e. a domain is normal iff its localisations at every maximal ideal is normal.

Good examples of such rings are unique factorisation domains. More generally, regular local rings are normal. The next best are two dimensional rings with an isolated singularity.

J.-P. Serre gave the following characterization of normal rings: A ring is normal iff it satisfies *the Serre's conditions* R_1 and S_2. What are these conditions? The condition R_1 means that for each prime $\mathfrak{p}$ of codimension one, $R_{\mathfrak{p}}$ is a discrete valuation domain. The condition S_2 means that every ideal of codimension two contains a regular sequence of R with two elements. In terms of associated primes, a ring is normal iff $\mathrm{Ass}\,(R)$ and $\mathrm{Ass}\,(R/(a))$, for every non-zero- divisor $a \in R$, have no embedded primes.

Due to the above criterion, one normally does the normalization of a ring in two steps: First one does S_2-ification and next, one desingularizes in codimension one. The reader will find details of such an approach in the book of W. Vasconcelos.

Here we describe an algorithm which goes back to Grauert and Remmert and was proposed by T. de Jong ([J]). This was further modified in a paper of Decker-Greul-Pfister-Jong. There are also algorithms by Gianni, Trager, by C. Traverso, and by W. Vasconcelos to compute the normalization.

First a preview: A criterion for normality states that $R = \overline{R}$ if and only if the canonical map $R \to \mathrm{Hom}_R(J, J)$ is an isomorphism, where J denotes a reduced ideal such that its zero set contains the non–normal locus of $\mathrm{Spec}\, R$. We shall prove this shortly.

Note: In general this map is only injective and one has an inclusion of rings,

$$R \subset \mathrm{Hom}_R(J, J) \subset \overline{R}.$$

The method is to present $\mathrm{Hom}_R(J, J)$ as an affine ring R_1, which is of type $R[T_1, \ldots, T_s]$ modulo an ideal generated by linear and quadratic relations in the T_i. One can continue in the same manner with R_1 and obtain a sequence of rings

$$R = R_0 \not\subseteq R_1 \not\subseteq \cdots \not\subseteq R_k = \mathrm{Hom}_{R_k}(J_k, J_k),$$

such that $R_k = \overline{R}$ by the criterion of Grauert and Remmert (the algorithm must stop, since $\overline{R}$ is finite over R).

Criterion for Normality

The alogrithm is based on the following criterion for normality:

Proposition *Let R be a noetherian reduced ring and J be a radical ideal containing a non-zero divisor such that the zero set of J, $V(J)$ contains the non-normal locus of $Spec(R)$. Then R is normal if and only if $R = Hom_{\ R}(J, J)$.*

Proof: Let $\overline{R}$ be the normalization of R. Then we have the canonical inclusions

$$R \subset \ \mathrm{Hom}_R(J,\ J) \subset \overline{R}$$

$$r \rightsquigarrow \varphi_r, \quad \varphi \rightsquigarrow \frac{\varphi(x)}{x}$$

where φ_r is the map defined by the multiplication with r and x is a non-zero divisor of J. It is easy to see that $\frac{\varphi(x)}{x}$ is independent of the choice of x. Since J is finitely generated, the characteristic polynomial o f φ defines an integral relation and, $\frac{\varphi(x)}{x} \in \overline{R}$.
Now we claim that

$$\mathrm{Hom}_{\ R}(J, J) = \mathrm{Hom}_R(J, R) \cap \overline{R}$$

Indeed, let $h \in \overline{R}$ and $h^n + a_{n-1}h^{k-1} + \cdots + a_0 = 0,\ a_i \in R$. If $h \in \mathrm{Hom}_R(J, R)$, that is $hJ \subset R$, then for all $g \in J$ we have $hg \in R$ and

$$(gh)^n + ga_{n-1}(gh)^{n-1} + \cdots + g^n a_0 = 0$$

which implies $(gh)^n \in J$. But J is a radical ideal and, therefore, $gh \in J$, which implies $h \in\ \mathrm{Hom}_R(J, J)$.
Now we are prepared for the proof of the proposition.
One implication is trivial. To prove the other, assume $R = \mathrm{Hom}_R(J, J)$. This implies $R = \mathrm{Hom}_R(J, R) \cap \overline{R}$.
Let $h = \frac{f}{g} \in \overline{R}$, it suffices to show that $hJ \subset R$.
Let

$$\Delta = \{P \in\ \mathrm{Spec}(R) \mid h \notin R_P\},$$

Δ is contained in the non-normal locus of $\mathrm{Spec}(R)$ and, therefore, by assunption $\Delta \subseteq V(J)$. Δ can be defined by the ideal

$$C = \{u \in R \mid hu \in R\}.$$

By the Nullstellensatz, we obtain $\sqrt{C} \supseteq J$. Now, by definition $h \cdot C \subseteq R$ and we may choose an integer d such that $R \supseteq h\sqrt{C}^d \supseteq hJ^d$. Assume that d is minimal s uch that $R \supseteq hJ^d$. If $d > 1$, then there exists an $a \in J^{d-1}$ such that $ha \notin R$ but $ha \in \overline{R}$ and $haJ \subset R$. This implies, because $\mathrm{Hom}_R(J, J) = \mathrm{Hom}_R(J, R) \cap \overline{R}$ that $ha \in J \subseteq R$, which gives a contradiction. Therefore, $d = 1$ and $hJ \subseteq R$, which proves the proposition.

Remark. Let $J,\ R$ be as in the Proposition and x a non-zero divisor, then

- $xJ : J = x.Hom_R(J,\ J)$, and, consequently,
- $R = Hom_R(J,\ J)$ if and only if $xJ : J \subseteq (x)$.

- Let $u_0 = x_1, u_1, \dots, u_s$ be generators of $xJ : J$. Because of the fact that Hom $_R(J, J)$ is a ring we have $\frac{s(s+1)}{2}$ relations

$$\frac{u_i}{x} . \frac{u_j}{x} = \sum_{k=0}^{s} \xi_k^{ij} \frac{u_k}{x}, \ s \geq i \geq j \geq 1, \ \xi_k^{ij} \in R$$

in $\frac{1}{x}(xJ : J)$, which together with the linear relations, the syzygies, betweem $u_o, \dots, u_s$, define the ring structure of $Hom_R(J, \ J)$:

$$[T_1, \dots, T_s] \overset{T_i \to \frac{u_i}{x}}{\to} Hom_R(J, J)$$

The kernel of this map is the ideal generted by the $T_iT_j - \sum_{k=0}^{s} \xi_k^{ij} \ T_{kj}$ where $T_0 = 1$, and $\sum_{k=0}^{s} \eta_k T_k$ such that $\sum_{k=0}^{s} \eta_k u_k = 0$.

Algorithm

NORMAL(I)

Input: a radical ideal $I \subseteq K[x_1, \dots, x_n]$,
Output: s polynomial rings $R_1, \dots, R_s$ and s prime ideals $I_1 \subset R_1, \dots, I_s \subset R_s$ and s maps $\pi_i : R \to R_j$, such that the induced map $\pi : K[x_1, \dots, x_n]/I \to R_1/I_1 \times \dots \times R_s/I_s$ is the normalization of $K[x_1, \dots, x_n]/I$.
- Result $= \emptyset$.
- Compute idempotents of $K[x_1, \dots, x_n]/I$;

Assume $K[x_1, \dots, x_n]/I = K[x_1, \dots, x_n]/I_1 \times \dots \times K[x_1, \dots, x_n]/I_s$.
- For $i = 1$ to s do

- Compute $J =$ singular locus of I_i.
- Choose $f \in J \backslash I_i$ and compute $I_i : f$ to check whether f is a zero divisor
- if $I_i \not\subset (I_i : f)$ then

Result = Result $\cup$
NORMAL $(\sqrt{I_i, \ f}) \cup$ NORMAL $(I_i : f)$
else
$J = \sqrt{I_i, f}$
$H = (fJ : J)$ if $H = \langle f \rangle$
Result = Result $\cup \{K[x_1, \dots, x_n], I_i, \ id\}$
else
assume $H = fJ : J = \langle f, u_1, \dots, u_s \rangle$
then compute an ideal $L \subseteq K[x_1, \dots, x_n, \ T_1, \dots, T_s]$ such that

$$K[x_1, \dots, x_n, \ T_1, \dots, T_s]/L \overset{\sim}{\to} Hom(J, J), \ T_i \to \frac{u_i}{f}$$

Let $\varphi : K[x_1, \dots, x_n] \to K[x_1, \dots, x_n, \ T_1, \dots, T_s]$ be the inclusion.
$S =$ normal (L);

Compose the maps of S with φ;
Result = Result $\cup S$;
• return Result

Finding zeros via Idempotents

We now describe an algorithm to compute the idempotents, atleast when the ideal I is homogeneous, as then the idempotents live in the zero-dimensional part.

We first study affine Artinian rings with the view towards determining their idempotents.

There are two ways of describing a commutative affine algebra of Krull dimension zero:

- $R = k[x_1, \cdots, x_n]/I$, where $I = (f_1, \cdots, f_r)$ is an ideal of codimension m;

- as a k-vector space basis $e_1, \cdots, e_n$, with attached *structure constants* $\{c_{ij}, 1 \leq i, j, \ell \leq n\}$, that is

$$e_i \cdot e_j = \sum_{\ell=1}^{n} c_{ij\ell} e_\ell$$

A Gröbner basis computation enables us to find the structure constants attached to the basis given by the standard monomials: If $\{m_1, \cdots, m_q\}$ are the standard monomials of some Gröbner basis, then $\mathrm{NormalForm}(m_i \cdot m_j) = \sum_{\ell=1}^{q} c_{ij\ell} m_\ell$. The second presentation has the obvious advantage that one can convert the problems into questions of linear algebra problems. We shall see an example of this shortly.

Note that if the structure constants are mostly non-trivial, then carrying them around can be cumbersome for large dimensions, and in such cases it may be preferable to work with the f_j's and to produce the structure constants directly from them also.

Generic Algebras. The relations that the structure constants c_{ijk} of an n-dimensional k-algebra A must satisfy are:

$$\begin{aligned} c_{ij\ell} &= c_{ji\ell} \quad \text{for the commutative law} \\ \sum_\ell c_{ij\ell} c_{\ell kp} &= \sum_\ell c_{jk\ell} c_{i\ell p} \quad \text{for the associative law} \\ c_{1j\ell} &= \delta_\ell^j \quad \text{for the identity element} \end{aligned}$$

Let A_n denote the algebra defined by the n^3 symbols $c_{ij\ell}$. Thus, $A_n = k[c_{ij\ell}, 1 \leq i, j, \ell \leq n]/I$, with I generated by the three sets of equations above. The k-rational points of the variety $V(I)$ are the n-dimensional commutative k-algebras.

Idempotents in Artin Algebras. Let R have finite dimension n over k, and let $\{e_1, \cdots, e_n\}$ be a basis of R over k, and the $\{c_{ij\ell}\}$ be the corresponding structure constants. Let $E = \sum_{i=1}^{n} x_i e_i$ be an idempotent of R, i.e. $E^2 = E$. (Here we think of x_i as the image of the indeterminates in R.) This will give rise to the following natural definition:

The solution in k^n of the n quadratic equations

$$f_\ell \;=\; \sum_{i,j} c_{ij\ell}x_ix_j - x_\ell,$$

for $1 \leq \ell \leq n$, is the *variety of idempotents of* R. The solutions are the idempotents of R.

The structure of this ideal is easy to describe:

Proposition Let $I = (f_1, \cdots, f_n) \subset k[x_1, \cdots, x_n]$ as above. Then I is a zero-dimensional radical ideal of S.

Proof. It is easy to see that the ideal I is independent of the chosen basis. It is also clear that we may extend the field k, so we may assume that it is algebraically closed. The algebra R breaks up into local Artin algebras $R = R_1, \times \cdots \times R_m$, where each R_i can be written as $R_i = k + M_i$, M_i being its radical. It suffices now to prove the assertion for each R_i. So assume $R = k + M$. Pick a basis of R over k, with $e_1 = 1$ and $e_i \in M$, for $i \geq 2$. The system of equations $f_\ell = 0$ has only two roots, corresponding to the trival idempotents 0 and 1: This follows from the fact that the Jacobian matrix $\partial(f_1, \cdots, f_n)/\partial(x_1, \cdots, x_n)$ has its diagonal elements equal $1 - 2x_1$, and the off-diagonal entries like in $(x_2, \cdots, d_n)$. Its determinant cannot vanish at any of these roots.

Thus, the above observation can be used to find all the idempotents of the given Artinian k-algebra.

4 Some basic Commutative Algebra

Primary Decomposition

Let M be a R- module. A prime ideal $\mathfrak{p}$ is said to be *associated* to M if $\mathfrak{p} = \mathrm{Ann}\,(M)$, for some $m \in M$. $\mathrm{Ass}\,(M)$ will denote the set of all associated primes of M. Equivalently, a prime ideal $\mathfrak{p} \in \mathrm{Ass}\,(M)$ iff $R/\mathfrak{p} \subseteq M$.

Note that if R is *noetherian* then $\mathrm{Ass}\,M = \emptyset$ iff $M = (0)$. This follows from the observation.

Lemma. An ideal I which is maximal amongst ideal of the form $\mathrm{Ann}\,(m)$, for $m \in M$, $m \neq 0$, is a prime ideal.

Proof. Let $ab \in I = \mathrm{Ann}\,(m)$, and $b \notin I$. Hence, $bm \neq 0$, and $a \in \mathrm{Ann}\,(bm) \subseteq ann(m) = I$.

Corollary. The homothesy $m_a : M \to M$ given by multiplication by $a \in R$ is injective iff a does not belong to any associated prime of M.

Proof. If $a \in \mathfrak{p} \in \mathrm{Ass}\ M$, then $R/\mathfrak{p} \subseteq M$, and $m_a|(R/\mathfrak{p}) \equiv 0$. Conversely, if $am = 0$, for some $m \neq 0$ in M, and $\mathfrak{p} \in \mathrm{Ass}\,(Rm)$ then $\mathfrak{p} = \mathrm{Ann}\,(r_0m)$, for some $r_0 \in R$. Hence, $ar_0m = 0$ implies that $a \in \mathfrak{p}$. But $\mathfrak{p} \in \mathrm{Ass}\,(M)$ also!

Corollary. The set of zero-divisors $Z(R)$ of a noetherian ring R is $\displaystyle\bigcup_{\mathfrak{p}\in \mathrm{Ass}\,(R)} \mathfrak{p}$. If M is a noetherian R-module then $Z(M) = \displaystyle\bigcup_{\mathfrak{p}\in \mathrm{Ass}\,(M)} \mathfrak{p}$.

We now study modules M which have a unique associated prime- these are called $\mathfrak{p}$-*primary* modules whee $\mathfrak{p}$ is the unique associated prime. More generally, one has a relative version:

A sub-module N of M is *primary* iff $m_a : M/N \to M/N$ is either injective or nilpotent. This is iff m_a is injective or $a^k M \subset N$ for some k. The set $\{a \mid m_a \ \ \textit{nilpotent}\}$ is easily verified to be a prime ideal $\mathfrak{p}$. We say N is $\mathfrak{p}$-primary submodule of M.

Clearly, $\mathfrak{p}$ is the unique element of $\operatorname{Ass}(M/N)$: For if $\mathfrak{p} \in \operatorname{Ass}(M/N)$, then $\mathfrak{p}_i = \operatorname{Ann}(\overline{m}_i)$, whence, m_x is not injective, for $x \in \mathfrak{p}_i$. But then m_x is nilpotent, and so $x \in \mathfrak{p}$ Conversely, if $x \in \mathfrak{p}$, and $x^k M \subset N$ then $x^k \in \operatorname{Ann}(M/N) \subset \operatorname{Ann} \overline{m}_i = \mathfrak{p}_i$. Hence, $x \in \sqrt{\mathfrak{p}_i} = \mathfrak{p}_i$, for any i.

Thus, M/N, is $\mathfrak{p}$-primary iff $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$.

Let R be a noetherian ring, and let M be a finitely generated R-module. Let N be a submodule of M. A *primary decomposition* of N is a finite family $\{Q_i\}$ of submodules of M which are $\mathfrak{p}_i$-primary with respect to M, and such that $N = \cap Q_i$.

A primary decomposition is said to be *irredundant* if "no $\mathfrak{p}_i$ can be dropped", i.e.

(i) if $\bigcap\limits_{j \neq i} Q_j \subseteq Q_i$, for any i.

(ii) If $\operatorname{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$ then $\mathfrak{p}_i \neq \mathfrak{p}_j$, if $i \neq j$.

Theorem (Existence of Primary Decomposition). Every submodule N of a finitely generated module M over a noetherian ring R has an irredundant primary decomposition.

Proof. If M/N is not primary then there is $a \in R$ such that $m_r : M/N \to M/N$ is neither injective nor nilpotent.

Let $N_1 = (N : r) \underset{\neq}{\supset} N$: the inclusion is proper as m_r is not injective.

The ascending chain

$$(N : r) \subseteq N : r^2) \subseteq \ldots (N : r^k) \subseteq \ldots$$

stops, say $(N : r^{k_0}) = (N : r^{k_0+1}) = \ldots$

Claim: $N = (N, r) \cap (N : r^{k_0})$.

For, if $mr^{k_0} \in N$, and $m = n + r^{k_0} m'$, then $r^{2k_0} m' \in N$, whence $m' \in (N : r^{2k_0}) = (N : r^{k_0})$. Hence, $r^{k_0} m' \in N$, and so $m = n + r^{k_0} m' \in N$.

We now use noetherian induction: Choose N to be maximal submodule which does not have a primary decomposition. Then M/N is not primary, and so $N = (M, r^{k_0}) \cap (N : r^{k_0})$, with $(N, r^{k_0}) \underset{\neq}{\supset} N$, $(N : r^{k_0}) \underset{\neq}{\supset} N$. By maximality of N, (N, r^{k_0}), $(N : r^{k_0})$ have a primary decomposition. But then so does N! A contradiction.

The irredundancy of the primary decomposition is clear by noting that if N_1, N_2 are $\mathfrak{p}$-primary with respect to M then so is $N_1 \cap N_2 : M/N_1 \cap N_2 \hookrightarrow M/N_1 \oplus M/N_2$, whence $\operatorname{Ass}(M/N_1 \cap N_2) \subseteq \operatorname{Ass}(M/N_1 \oplus M/N_2) = \{\mathfrak{p}\}$ (Check the last equality !)

Corollary. If M is a f.g. module over a noetherian ring then $\operatorname{Ass}(M)$ is a finite set $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$.

Proof. If $(0) = \bigcap\limits_{i=1}^{r} N_i$, with N_i $\mathfrak{p}_i$- primary is an irredundant primary decomposition then $\operatorname{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Remark. The minimal primes of $\operatorname{Ass}(M)$ are called *minimal* (or isolated) prime of M. They correspond to the maximal points of $\operatorname{Supp}(M)$. Those primes which are not minimal are called *embedded primes.*

1. A constructive method to get primary decomposition of monomial ideals: Let M be a monomial ideal of $k[x_1, \cdots, x_n]$. If u, v are relatively prime monomials, then show that $(M, uv) = (M, u) \cap (M, u)$. Use this to get a primary decomposition of (x^2yz, y^2z, yz^3)

2. Prove that a monomial ideal is primary iff there is a subset $\{x_{i_1}, \ldots, x_{i_r}\} \subseteq \{x_1, \ldots, x_n\}$ such that I is generated by monomials in the x_{i_j} and contains a power of each of these variables. In particular, every irreducible monomial ideal is generated by powers of a subset of the indeterminates.

3. Justify the folowing algorithm to compute primary decomposition of a monomial ideal: Let I be an ideal generated by the set of monomials $L = \{f_1, \cdots, f_m\} \subset k[x_1, \cdots, x_n]$.
   - If there is a power of each $x_i \in L$, then I is primary.
   - If a variable, say x_n, occurs in some f_i but does not occur as a simple power in L, let x_n^s be the largest power of x_n that appears as a factor. Then $I = (I, x_n^2) \cap (I : x_n^s)$.
   - Repeat the previous two steps on (I, x_n^s) and on $(I : x_n^s)$.
   - Return a primary decomposition of I.

Schanuel's Lemma

Lemma: (Schanuel)
If P, P' are projective A-modules and you have exact sequences of A-modules,

$$\begin{array}{ccccccccc} 0 & \to & K & \to & P & \xrightarrow{\alpha} & M & \to & 0 \\ & & & & & & \| & & \\ 0 & \to & K' & \to & P' & \xrightarrow{\beta} & M & \to & 0 \end{array}$$

then $P' \oplus K \simeq P \oplus K'$.

Proof: Since P, P' are projective one has R-linear map f, g so that

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & P \arrow[r, "\alpha"] \arrow[d, shift left, "f"] & M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & K' \arrow[r] & P' \arrow[r, "\beta"] \arrow[u, shift left, "g"] & M \arrow[r] & 0 \end{tikzcd}$$

$\beta f = \alpha$, $\alpha g = \beta$.
Let $X \subset P \oplus P'$ be the pull-back of α, β, i.e.

$$X = \{(p, p') \in P \oplus P' : \alpha(p) = \beta(p')\}.$$

One has the diagram

$$
\begin{tikzcd}
0 \arrow[dr] & & & & 0 & \\
& K \arrow[dr] & & P \arrow[ur] \arrow[dr, "\alpha"] \arrow[dl, shift left] & & 0 \\
& & X \arrow[ur, "p_1", shift left] \arrow[dr, "p_2"', shift right] & & M \arrow[ur] \arrow[dr] & \\
& K' \arrow[ur] & & P' \arrow[ur, "\beta"'] \arrow[dr] \arrow[ul, shift right] & & 0 \\
0 \arrow[ur] & & & & 0 &
\end{tikzcd}
$$

Here p_1, p_2 are the natural projections which are onto as α, β are onto maps. Their kernels are K', K respectively. Since P, P' are projective the crossed exact sequences splits. Hence $P \oplus K' \simeq X \simeq P' \oplus K$.

Homological dimension of f.g. modules

The concept of homological dimension $hd_R M$ of a f.g. R-module M is a measure of how far a f.g. R-module is from being projective. Therefore one takes that a f.g. projective module is the simplest type, i.e. $hd_R P = 0$ and one has $hd_R M = 0$ if and only if M is R-projective. One studies other R-modules in terms of the projective R-module.

Any f.g. module M is the image of f.g. free module F

$$0 \to K \to F \to M \to 0$$

Let K be the kernel. The next simplest modules are those for which K is projective. Note that if for some free module F and some map $F \to M \to 0$ one has K projective then for any other free module F' and surjection $F' \to M \to 0$, with kernel K', we will have K' projective! This is a consequence of Schanual's lemma :

$$
\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & K' \arrow[r] & F' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}
$$

One has $F \oplus K' \simeq F' \oplus K$, and so K' is projective. We will say above that $hd_R M = 1$.

More generally we say that $hd_R M = n$ if there is an exact sequence (called projective resolution of length n) of f.g. projective R-modules $P_i, 0 \leq i \leq n$, and maps

$$0 \to P_n \to P_{n-1} \to \cdots\cdots \to P_0 \to M \to 0,$$

and no such sequence of smaller length. By Schanuel's lemma it will follow that if $hd_R M = n$, and one had a sequence as above with P_i R-projective for $0 \leq i \leq n-1$, then necessaarily P_n must be R-projective.

If no such integer n exists we say that $hd_R M$ is infinite.

Examples:

(i) $hd_R M = 0$ if and only if M is R-projective.

(ii) $hd_R M = 1$ if and only if M is not R-projective and $M \simeq P/Q$, with P, Q projective.

(iii) Let a be a n.z.d. of R then $hd_R R/(a) = 1$ as one has a free resolution

$$0 \to R \simeq Ra \to R \to R/(a) \to 0.$$

Moreover since $ann\ R/(a) = (a) \neq 0$, $R/(a)$ is not R-projective.

(iv) Let $R = \mathbf{Z}_4$ and $I = (\overline{2})R$. Then $hd_R I = \infty$ as one has an exact sequence

$$0 \to I \to R \to I \to 0.$$

Note that $ann\ I \neq 0$, so I is not R-projective. Hence $hd_R I \neq 1$. Again, one has an exact sequence, $0 \to I \to R \to R \to I \to 0$

$$\begin{tikzcd}
& 0 \arrow[r] & I \arrow[r] & R \arrow[r] & I \arrow[r] & 0 \\
& & R \arrow[u] \arrow[ur] & & & \\
& I \arrow[ur] & & & & \\
0 \arrow[ur] & & & & &
\end{tikzcd}$$

Therefore, $hd\ I \neq 2$. In this way it is clear that $hd_R I \neq n$ for any n.

(v) More generally, let R be an Artinian local ring. Then for any f.g. R-module M either $hd_R M = 0$ or $hd_R M = \infty$. (Details left to the reader).

The key lemma used actually to compute homological dimension of a R-module M is

Lemma Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Then

$$hd\ M \leq Max(hd\ M', hd\ M'')$$

with equality except possibly when $hd\ M'' = hd\ M' + 1$.

Proof: One first claim that if any two of $hd\ M, hd\ M', hd\ M''$ is finite then so is the third : If M is projective M'' is projective then the result is easy to see. So assume $hd\ M > 0$, $hd\ M'' > 0$, and let $M = P/Q$, with P projective. Therefore, $M' = Q'/Q$ with $Q \subset Q' \subset P$, and $M'' \simeq P/Q'$. Now $hd\ Q' = hd\ M'' - 1$, $hd\ Q = hd\ M - 1$. One has the exact sequence

$$0 \to Q \to Q' \to Q'/Q = M' \to 0.$$

If we induct on the sum of the two finite homological dimension in an exact sequence then we get the claim. Now induct on the sum of all three finite homological dimension ! By induction one gets

$$hd\ Q' \leq Max(hd\ Q, hd\ M')$$

with equality except possibly when $hd\ M' = hd\ Q + 1$. Therefore,

$$hd\ M'' - 1 = Max(hd\ M - 1, hd\ M')$$

with equality except possibly when $hd\ M' = hd\ M$. Thus,

$$hd\ M \leq Max(hd\ M', hd\ M'')$$

with equality except possibly when $hd\ M'' = hd\ M' + 1$ (by considering the various possibilities which may occur).

Remark: The above lemma is most useful to compute $hd\ M''$ from $hd\ M'$ and $hd\ M$. This is sucessful except in the case when $hd\ M' = hd\ M$; then it is ambiguous as one only gets an inequality.

We note that homological dimension of a module is a "local property" i.e. to compute $hd_R M$ one may assume that R is a local ring to begin with. This is due to

Lemma: $hd\ M = \sup hd\ M_\wp$, $\wp \in SpecR$.

Proof: Let r.h.s. $= d$. Note that $hd_{R_\wp} M_\wp \le hd_R M$, and so $d \le hd_R M$. So if d is infinite then $hd_R M$ is infinite. Let us consider an exact sequence

$$0 \to K_d \to F_{d-1} \to \cdots \to F_0 \to M \to 0$$

with F_i free R-module. Then $(K_d)_m$ is free R_m-module. By ( ) K is projective, and so $hd\ M \le d$.

Lemma: Let x be a non-zero-divisor of R and M. Then

$$hd_R M = hd_{R/(x)} M/xM.$$

Proof: Choose an exact sequence

$$0 \to k \to F \to M \to 0$$

with F f.g. free R-module. Multiplication by x yields a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow x & & \downarrow x & & \downarrow x & & \\ 0 & \longrightarrow & k & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

By Snake lemma we get an exact sequence

$$0 \to K' \to F' \to M' \to K/xK \to F/xF \to M/xM \to 0,$$

with $M' = (M : x)$, etc. Since x is a n.z.d. on M, we have $M' = 0$, and an exact sequence

$$0 \to K/xK \to F/xF \to M/xM \to 0. \qquad (*)$$

Again, $F' = 0$, and so $K' = 0$, i.e. x is a n.z.d. on K.

We may assume that one of the $hd_R M, hd_{R/(x)} M/xM$ is finite. Assume the former; a similar argument can be done in the latter case. Let $hd\ M = m$; then $hd\ K = m - 1$. By induction on $hd_R M$, we may assume $hd_{R/(x)} K/xK = hd_R K = m - 1$.

Suppose M/xM is free. Choose a resolution $(*)$ with F free of rank $=$ rank M/xM. Then $K/xK = 0$ and via Nakayama's lemma $K = 0$, whence $M \simeq F$ is free.

If $hd_{R/(x)} M/xM \ne 0$, then $hd_{R/(x)} M/xM = hd_{R/(x)} K/xK + 1 = hd_R K + 1 = hd_R M$; as required.

Finally, we mention without proof, the celebrated theorem of Aüslander-Serre

Theorem: A ring R is regular if and only if it has finite homological dimension.

Regular R-sequences

In this we introduce the notion of a regular sequence of elements of R. In general, these are a set of elements which are in a nice general position, as each avoids being in the union of the associated primes containing the previous ones. The set of indeterminates $x_1, \cdots, x_n$ in a polynomial ring is a typical example; and in general, when one has a regular sequence of elements, they behave, in some sense, like the variables. A major problem is how to obtain a set of regular elements in a ring in a constructive manner.

Let M be an R-module. Then an ordered sequence $\{a_1, \cdots, a_n\}$ of R is said to be a regular M-sequence if

1. $(a_1, \ldots, a_n)M \neq M$
2. $a_i \notin Z(M/(a_1, \ldots, a_{i-1})M)$, for all $1 \leq i \leq n$. Thus, a_1, is non-unit, non-zero divisor on M, a_2 is non-unit, non-zero divisor on M/a_1M, etc. if M is noetherian overa noetherian ring R. (Here $Z(M)$ denotes the set of zero-divisors of M.)

Remark. The order is imporant. For instance, $R = k[x,\ y,\ z]$, $a_1 = x(y-1)$, $a_2 = y$, $a_3 = z(y-1)$. Then, $a_1,\ a_2,\ a_3$ is a R- regular sequence, whereas $a_1,\ a_3\ a_2$ is not.

Exercise. Give an example where $a_1,\ a_2$ is a regular sequence, where $a_2,\ a_1$ is not !

Depth and Associated Primes

Let R be a Noetherian ring, I an ideal in R, M a finitely generated R-module, satisfying $IM \neq M$. Then any two maximal R-sequences on M contained in I have the same length. This length is called the **grade** of I on M. If $M = R$, is a local ring with maximal ideal $\mathfrak{m}$, then the grade of $\mathfrak{m}$ on R is called the **depth** of the ring R. This is an important numerical invariant of a ring R.

The aim of the this subsection is to show that a f.g. R-module M over a noetherian local ring R has $depth(M) \leq \dim R/p$, for all $p \in \mathrm{Ass}\,(M)$. We first input a simple observation.

Lemma. Let R be a noetherian ring, and M a finitely generated R-module. Let $x \in A$ be a M=regular element with $\displaystyle\bigcap_{n\geq 1} x^n M = (0)$. Let $\mathfrak{p} \in \mathrm{Ass}\,(M)$. Then there is a $\mathfrak{q} \in \mathrm{Ass}\,(M/xM) \cap V(\mathfrak{p} + xR)$.

Proof. Let $\mathfrak{p} = \mathrm{Ann}\,(m_0)$ for some $m_0 \in M$. Choose r so that $m_0 \in x^r M \backslash x^{r+1}M$. Let $m_o = x^r m_1$, $m_1 \in M\backslash xM$. Now $\mathrm{Ann}\,(m_1) = \mathrm{Ann}\,(m_0)$. Now $(\mathfrak{p}+xR)\overline{m}_1 = 0$. Hence, there is $\mathfrak{q} \in \mathrm{Ass}\,(M/xM)$ such that $\mathfrak{p} + xR \subseteq \mathfrak{q}$.

Proposition (Depth and Associated Primes)

Let $(R, \mathfrak{m})$ be a local ring, and let M be a non-zero finitely generated R-module. Then $depth(M) \leq \dim(A/\mathfrak{p})$, for every $\mathfrak{p} \in \mathrm{Ass}\,(M)$. In particular, $depth(M) \leq \dim(M)$.

Proof. Induct on $\dim(R/\mathfrak{p})$. If $\dim(R/\mathfrak{p}) = 0$, then $\mathfrak{p} = m \in \mathrm{Ass}\,(M)$. hence, $depth(M) = 0$.

Let $depth(M) > 0$. Let $x \in m$ be M-regular, and let $M_1 = M/xM$. By Lemma above find $\mathfrak{q} \in \mathrm{Ass}\,(M_1)$ with $\mathfrak{q} \supseteq \mathfrak{p} + xR$. By the induction hypothesis, $depth(M_1) \leq$

$\dim(R/\mathfrak{p})$. But $depth(M_1) = depthM - 1$, and $\mathfrak{q} \underset{\neq}{\supset} \mathfrak{p}$ implies $\dim(R/\mathfrak{q}) < \dim(R/\mathfrak{p})$. Hence, $depth(M) \leq \dim(R/\mathfrak{p})$ and induction prevails.

Cohen-Macaulay Modules

We know that depth $(M) \leq \dim(M)$, which is the Krull dimension of $R/\mathrm{Ann}(M)$, for any finitely generated module M over a noetherian ring. The case of equality has much significance, and is given a special name.

Let $(R, \mathfrak{m})$ be a noetherian local ring, and M be a finitely generated R-module. We say that M is **Cohen-Macaulay** (C.M. in short) if $M = 0$ or if

$$\operatorname{depth}(M) = \dim(M).$$

If the local ring $(R, \mathfrak{m})$ is Cohen-Macaulay as a R-module, then we say that R is a Cohen-Macaulay ring.

Some properties of Cohen-Macaulay modules are listed below:

1. A Cohen-Macaulay module has no embedded primes.

   Proof: depth $(M) = \dim(M) = \dim(R/\mathrm{Ann}(M) \geq \dim(R/\mathfrak{p} \geq \operatorname{depth}(M)$.

2. If $a_1, a_2, \cdots, a_r$ is an M-regular sequence in $\mathfrak{m}$, then $M_r = M/(a_1, \cdots, a_r)M$ is also C.M. of depth r less than the depth of M.

   Proof: Verify this.

3. For every prime ideal $\mathfrak{p}$ of R, $M_{\mathfrak{p}}$ is C.M.

   Proof: If $M \neq 0$ then $\mathrm{Ann}(M) \subseteq \mathfrak{p}$. We induct on $d = \operatorname{depth}_{\mathfrak{p}} M$. If $d = 0$ then $\mathfrak{p} \subset \mathfrak{q}$, for some $\mathfrak{q} \in \mathrm{Ass}(M)$. Since the associated primes of M are all minimal, we get $\mathfrak{q} = \mathfrak{p}$, whence $\dim M_{\mathfrak{p}} = \operatorname{height}(\mathfrak{p}/\mathrm{Ann}(M) = 0$. If $\operatorname{depth}_{\mathfrak{p}}(M) > 0$, take an M-regular element $a \in \mathfrak{p}$, and put $M_1 = M/aM$. Then $a_{\mathfrak{p}}$ is $M_{\mathfrak{p}}$-regular, whence $\operatorname{depth}(M/aM)_{\mathfrak{p}} = \operatorname{depth} M_{\mathfrak{p}} - 1$, and $\dim(M/aM)_{\mathfrak{p}} = \dim(M_{\mathfrak{p}}/aM_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}} - 1$. Since $M/aM$is C.M., by induction we conclude that $\operatorname{depth}(M/aM)_{\mathfrak{p}} = \dim(M/aM)_{\mathfrak{p}}$. This shows that $M_{\mathfrak{p}}$ is C.M.

4. For any proper ideal I of a C. M. ring $(R, \mathfrak{m})$ we have

   $$height\ (I) + dim\ (R/I) = dim\ (R)$$

   Proof: It suffices to prove this for a prime ideal $\mathfrak{p}$. Let *height* $(\mathfrak{p}) = r$. Since $R_{\mathfrak{p}}$ is C.M. $\operatorname{depth}_{\mathfrak{p}} = r$. Let $a_1, \cdots, a_r$ be a regular sequence in $\mathfrak{p}$. Then $R/(a_1, \cdots, a_r)$ is C.M. of dimension $d - r$, where d is the dimension of R. But then the minimal prime ideal $\mathfrak{p}$ of $R/(a_1, \cdots, a_r)$ has $\dim(R/\mathfrak{p}) = \operatorname{depth} R/(a_1, \cdots, a_r) = n - r$.

M-Regular Sequences and Higher Ext.

In this section we treat the grade of M with respect to I by an alternative approach. The information gleaned is useful to us later.

Lemma. Let R be a noetherian ring, I an ideal, M a finitely generated R-module. Then, the following are equivalent.

(i) There exists a M-regular sequence $a_1, \dots, a_n$ in I.

(ii) $\text{Ext}^i(R/I, M) = 0$ for $i < n$,

(iii) $\text{Ext}^i(N.M) = 0$, for any R-module N with Supp $(N) \subseteq V(I)$, and for $i < n$.

Proof: (iii) $\Rightarrow$ (ii) is trivial.

(ii) $\Rightarrow$ (i) : we have $Ext^0(R/I, M) = Hom_R(R/I, M) = 0$. If no element of I is M-regular then $I \subseteq \bigcup_{\mathfrak{p} \in Ass(M)} \mathfrak{p}$. Hence, $I \subseteq \mathfrak{p}_0$, for some $\mathfrak{p}_0 \in Ass(M)$. hence, $R/p_o \hookrightarrow M$, and the natural map $R/I \hookrightarrow R/\mathfrak{p}_0 \hookrightarrow M$ shows that $Hom(R/I, M) \neq 0$, a contradiction. Hence, there is $a_1 \in I$ which is M-regular. Let $n > 1$, and let $M_1 = M/a_1M$. We have the exact sequence.

$$0 \to M \stackrel{a_1}{\to} M \to M_1 \to 0$$

The associated long exact sequence of cohomology is

$$\cdots \to Ext^i(R/I, M) \to Ext^i(R/I, M_1) \to Ext^{i+1}(R/I, M) \to \cdots$$

By assumption, $Ext^i(R/I, M) = 0$, for $i < n$. Hence, $Ext^i(R/I, M_1) = 0$, for $i < n - 1$. By induction on n there exists a M_1- regular sequence $a_2, \dots, a_n$ in I. Thus, $a_1, \dots, a_n$ is a M-regular sequence in I.

(i) $\Rightarrow$ (iii): Let $M_1 = M/a_1M$. By induction on n, $Ext^i(N, M_1) = 0$, for $i < n - 1$. We have the exact sequence $0 \to M \stackrel{a_1}{\to} M \to M_1 \to 0$ induces the long exact sequence of cohomology,

$$\cdots \to Ext^{i-1}(N, M) \to Ext^i(N, M) \stackrel{a_1}{\to} Ext^i(N, M) \to \cdots .$$

Hence, $0 \to Ext^i(N, M) \stackrel{a_1}{\to} Ext^i(N, M)$ is exact for each $i < n$. Since $Supp\ (N) \subseteq V(ann(N)) \subseteq V(I)$, we get $I \subseteq \sqrt{ann(N)}$. Hence, $a_1^r \in ann(N)$, for some $r > 0$. Hence, $a_1^r \in ann(Ext^i(N, M))$. Thus, $Ext^i(N, M) = 0$ for $i < n$!

Corollary: The length of a maximal M-regular sequence in I depends only on M and I, and equals the number n such that

$$Ext^i_R(R/I, M) = \begin{cases} 0 & i < n \\ \neq 0 & i = n \end{cases}$$

Proof: We show that if $a_1, \dots, a_n$ is a M-regular sequence in I, then $\text{Ext}^n_R(R/I, M) \neq 0$. We induct on n. We have an exact sequence, $0 \to M \stackrel{a_1}{\to} M \to M/a_1M \to 0$. The long exact sequence of cohomology gives

$$\cdots \to \text{Ext}^{n-1}(R/I, M) \to \text{Ext}^{n-1}(R/I, M/a_1M) \to \text{Ext}^n(R/I, M) \to \cdots$$

By induction, $\text{Ext}^{n-1}(R/I, M/a_1M) \neq 0$ and $\text{Ext}^{n-1}(R/I, M) = 0$, hence
$\text{Ext}^{n-1}()R/I, M/a_1M) \subseteq \text{Ext}^n(R/I, M)$, which is therefore non-zero.

Homological Dimension and Depth

Definition: *$grade_I M$ is the least integer n* such that $\operatorname{Ext}^n_R(R/I, M) \neq 0$. If R is a local ring with $\mathfrak{m}$ its unique maximal ideal then $grade_{\mathfrak{m}} M$ is called *depth of M*. This equals the length of any maximal regular M-sequence in I.

The important Auslander-Buchsbaum theorem for modules of finite homological dimension relates its homological dimension with its depth.

Theorem (Aüslander and Buchsbaum)

Let (R, m) be a noetherian local ring, and M be a non-zero finitely generated R-module having a finite homological dimension. Then,

$$hdM + \ depth\ M = depth\ R.$$

Proof. We induct on $hd(M)$. If $hd(M) = 0$ then M is a projective R-module. Since R is local, $M \xrightarrow{\sim} R^k$ is free. Hence, $depth\ M = \ depth\ R^k = \ depth\ R$, as required. Let now $hd(M) = 1$, and let

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

be a minimal resolution of M. (In particular, $\varphi \in M_{m,n}(m)$, where $\mathfrak{m}$ is the maximal ideal of R.

The long exact sequence of cohomology is

$$\cdots \to \operatorname{Ext}^i(k, R^m) \xrightarrow{\varphi_*} \operatorname{Ext}^i(k, R^n) \xrightarrow{\tau_*} \operatorname{Ext}^i(k, M) \to \cdots$$

(Here, $k = R/\mathfrak{m}$). Observe that

$$\operatorname{Ext}^i(k, R^m) = \operatorname{Ext}^i(k, R)^m \xrightarrow{\varphi_*} \operatorname{Ext}^i(k, R)^n = \operatorname{Ext}^i(k, R^n)$$

is the matrix φ! Since $\mathfrak{m} \subseteq \operatorname{Ann}\ (\operatorname{Ext}^i(k, R^m))$, $\varphi_* = 0$. Hence, we get

$$0 \to Ext^i(k, R)^n \to Ext^i(k, M) \to Ext^{i+1}(k, R)^m \to 0$$

for every i. But $\operatorname{depth}(M) = \min\{i \mid \operatorname{Ext}^i(k, M) \neq 0\}$, whence $\operatorname{depth}(M) = \operatorname{depth}(R) - 1$.

In the general case, take any exact sequence

$$0 \to M \to R^n \to M' \to 0,$$

and note that $hd(M') = hd(M) - 1$. Now write the long exact sequence of cohomology,

$$\cdots \to \operatorname{Ext}^i(k, M') \to \operatorname{Ext}^i(k, R)^n \to \operatorname{Ext}^i(k, M) \to \cdots$$

By induction, $\operatorname{depth}(M') + \operatorname{hd} M - 1 = \operatorname{depth}(R)$. Hence, above exact sequence shows that $\operatorname{depth}(M) \geq \operatorname{depth}(M') - 1$ as $\operatorname{Ext}^i(k, M) = 0$ if $i < \operatorname{depth}\ (M') - 1$: Moreoever, for $i = \operatorname{depth}(M') - 1, \operatorname{Ext}^i(R, M) \xrightarrow{\sim} \operatorname{Ext}^{i+1}(k, M') \neq 0$. Hence, $\operatorname{depth}(M) = \operatorname{depth}(M') - 1$, as required.

A Lemma of Rees

Let N, M be R-modules, such that $a_1, \dots, a_n \in R$ is an N-sequence and $(a_1, \dots, a_n) \subseteq \mathrm{Ann}\,(M)$. Then

$$\mathrm{Ext}\,^n_R(M, N) \xrightarrow{\sim} \mathrm{Hom}\,_R(M, N/(a_1, \dots, a_n)N).$$

Proof: We prove the lemma by induction on n. Let $n \geq 1$, then we have an exact sequence

$$0 \to N \xrightarrow{a_1} N \to N/a_1N \to 0$$

of R-modules. This gives the long exact sequence

$$\to \mathrm{Ext}\,^{n-1}_R(M, N) \to \mathrm{Ext}\,^{n-1}_R(M, N/a_1N) \to \mathrm{Ext}\,^n_R(M, N)$$

$$\xrightarrow{a_1} \mathrm{Ext}\,^n_R(M, N) \to .$$

Since the last map is multiplication by a_1, and $a_1 \in \mathrm{Ann}\,(M) \subseteq \mathrm{Ann}\ \ \mathrm{Ext}\,^n(M, N)$, it is a zero map. Also, by induction

$$\mathrm{Ext}\,^{n-1}_R(M, N) \simeq \mathrm{Hom}\,(M, N/(a_1, \dots, a_{n-1})N).$$

Therefore, as $a_n \in \mathrm{Ann}\,(M)$ and a_n is a non zero-divisor on $N/(a_1, \dots, a_{n-1})N$, by the lemma given below, we have $\mathrm{Ext}\,^{n-1}(M, N) = 0$. Hence

$$\mathrm{Ext}\,^n(M, N) \simeq \mathrm{Ext}\,^{n-1}_R(M, N/a_1N) \simeq \mathrm{Hom}\,(M, N/(a_1, \dots, a_n)N),$$

where the last isomorphism is again by induction. This proves the lemma.

Lemma: Let M, N be R-modules. If there is $x \in \mathrm{Ann}\,(M)$, which is a non zero-divisor on N, then $\mathrm{Hom}\,_R(M, N) = 0$.

Proof: Let $f \in \mathrm{Hom}\,_R(M, N)$. Then, for any $m \in M$, we have $xf(m) = f(xm) = f(0) = 0$, which implies $f(m) = 0$ as x is a non-zero-divisor on N. Therefore $\mathrm{Hom}\,_R(M, N) = 0$.

An interesting consequence of Rees' lemma is the following corollary.

Corollary: Any two maximal regular M-sequence in I have the same length.

Proof: Suppose there are two M-sequences $a_1, \dots, a_n$ and $b_1, \dots, b_m$ in I such that $m > n$. Then

$$\mathrm{Ext}\,^n(R/I, M) \simeq \mathrm{Hom}\,(R/I, M/(a_1, \dots, a_n)M) \neq 0,$$

as $I \subseteq \mathbf{p}$ for some $\mathbf{p} \in \mathrm{Ass}\,(M/(a_1, \dots, a_n)M)$, which implies that there exists an injective map $R/\mathbf{p} \hookrightarrow M$ and hence the composite $R/I \longmapsto R/\mathbf{p} \hookrightarrow M$ is a non zero map. But on the other hand, by Lemma above,

$$\mathrm{Ext}\,^n(R/I, M) \simeq \mathrm{Hom}\,(R/I, M/(b_1, \dots, b_n)M) = 0.$$

Therefore $m = n$.

Corollary (Associated primes of $Ext^r(M, R)$**)**

Let R be a regular ring, and let M be a finitely generated R-module. Suppose that $\mathrm{Ann}\,(M)$ has codimension R. Then $Ext^r(M, R)$ is non-zero, and all of its associated primes are of codimension r.

Proof. By Rees' Lemma,

$$\mathrm{Ext}^{r}(M,R) \xrightarrow{\sim} Hom_{R/(x)}(M,\ R/(x)),$$

where (x), is a regular sequence of length r in R, contained in $\mathrm{Ann}\,(M)$. (Such a sequence will exist, say via **Prime Avoidance**.)

Now the associated primes of $M^* = Hom_{R/(x)}(M, R/(x))$ are all of codimension equal to *depth* (M^*), as $R/(x)$ is Cohen-Macaulay, and M^* is a finitely generated $R/(x)$- module.

5 Computational Primary Decomposition

Higher $\mathrm{Ext}^{n}(M.R)$ **and Associated primes** $\mathrm{Ass}\,(M)$**.**

Definition: For a finitely generated module M over a Noetherian ring, the *equidimensional hull of* 0 *in* M is the intersection of primary components of maximal dimension i.e. of $\dim(M)$. For an ideal I, by *hull of* I we mean the equidimensional hull of R/I.

Lemma: Let $(R, \mathfrak{m})$ be a regular local ring of dimension e, let N be an R-module of finite length. Then there exists an isomorphism of R-modules

$$N \longrightarrow \mathrm{Ext}^{e}_{R}(\mathrm{Ext}^{e}_{R}(N,R),R).$$

Proof: Since N is a module of finite length, depth $(N) = 0$. Therefore, by Aüslander-Buchsbaum, $\mathrm{hd}_{R}(N) = e$. Let

$$\mathcal{F} : \imath \longrightarrow \mathcal{F}_{\rceil} \xrightarrow{\phi_{\rceil}} \cdots \xrightarrow{\phi_{\in}} \mathcal{F}_{\infty} \xrightarrow{\phi_{\infty}} \mathcal{F}_{\imath} \xrightarrow{\phi_{\imath}} \mathcal{M} \longrightarrow \imath$$

be a projective resolution of N. By Rees's lemma, if $\{x_1, \ldots, x_e\}$ is an R-sequence in $\mathrm{Ann}\,(N)$ then

$$\mathrm{Ext}^{i}_{R}(N,R) \simeq \mathrm{Hom}\,(M, R/(x_1,\ldots,x_i)) = 0,$$

for all $i < e$. Therefore the dual of the resolution $\mathcal{F}$ is a free resolution for $\mathrm{Ext}^{e}_{R}(N,R)$, namely

$$\mathcal{F}^* : \qquad 0 \longrightarrow F_0^* \xrightarrow{\phi_1^*} F_1^* \xrightarrow{\phi_2^*} \cdots \longrightarrow F_{e-1}^* \xrightarrow{\phi_e^*} F_e^* \longrightarrow \mathrm{Ext}^{e}_{R}(N,R) \longrightarrow 0.$$

Hence

$$\mathrm{Ext}^{e}_{R}(\mathrm{Ext}^{e}_{R}(N,R),R) \simeq \mathrm{Hom}\,(F_0^*,R)/\mathrm{Im}\ \mathrm{Hom}\,(F_1^*,R).$$

If $\phi_1^{**} : \mathrm{Hom}\,(F_1^*,R)^* \to \mathrm{Hom}\,(F_0^*,R)^*$ is the map induced by ϕ^* then we have the following commutative diagrams

$$\begin{array}{ccc}
\mathrm{Hom}\,(F_1^*,R)^* & \xrightarrow{\phi_1^{**}} & \mathrm{Hom}\,(F_0^*,R)^* \\
{\scriptstyle f_0}\uparrow & & \uparrow{\scriptstyle f_0} \\
F_1 & \xrightarrow{\phi_1} & F_0,
\end{array}$$

where the canonical maps f_1 and f_0 are isomophisms as F_1 and F_0 are free R-modules. This implies that

$$\mathrm{Hom}\,(F_0^*, R)^*/\mathrm{Im}\ \mathrm{Hom}\,(F_1^*, R)^* \simeq F_0/\mathrm{Im}\ F_1 \simeq M.$$

Hence the lemma.

Theorem: Let M be a finitely generated module over a regular domain R. Let $I_e = \mathrm{Ann}\ \mathrm{Ext}\,^e_R(M, R)$. Then

1. codimension $I_e \geq e$,
2. $\mathrm{Ass}\,(M) \cap$ {primes of height e} $= V(I_e) \cap$ {primes of height e} and
3. $M/(0 : I_e)$ has no associated prime of codimension e.

Proof: It is enough to prove the assertions after localizing at each prime of height e, therefore one can assume that R is regular local ring of dimension e with maximal ideal $\mathbf{m}$.

1. By Aüslander-Buchsbaum theorem $\mathrm{hd}\,_R(M) \leq e$, which implies $\mathrm{Ext}\,^i(M, R) = 0$, for all $i > e$. Let

$$M' := H^0_{\mathfrak{m}}(M) = \{m \in M \mid \mathfrak{m}^n m = 0, \quad \text{for some} \quad n\},$$

so M' is the largest submodule of finite length in M. Now we prove that depth $(M/M') > 0$: If $\mathfrak{m} \in \mathrm{Ass}\,(M/M')$ then for some nonzero $\bar{m} \in M/M'$, we have $\mathfrak{m}(\bar{m}) = 0$ in M/M'. Therefore if m is a preimage of $\bar{m}$ in M, then $\mathfrak{m}(m) \subseteq M'$, which implies $m \in M'$, contradicting the hypothesis on $\bar{m}$. Hence depth $(M/M') > 0$.

Now consider the short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M/M' \longrightarrow 0.$$

of R-modules. This gives the long exact sequence of cohomology

$$\longrightarrow \mathrm{Ext}\,^e_R(M/M', R) \longrightarrow \mathrm{Ext}\,^e_R(M, R) \longrightarrow \mathrm{Ext}\,^e_R(M', R) \longrightarrow \mathrm{Ext}\,^{e+1}_R(M, R) \longrightarrow .$$

Since depth $(M/M') > 0$, by Aüslander-Buchsbaum we have $\mathrm{hd}\,_R(M/M') < e$, which implies $\mathrm{Ext}\,^i_R(M/M', R) = 0$, for $i \geq e$. Therefore $\mathrm{Ext}\,^e_R(M, R) \simeq \mathrm{Ext}\,^e(M', R)$. Hence $I_e = \mathrm{Ann}\ \mathrm{Ext}\,^e_R(M, R) = \mathrm{Ann}\,\mathrm{Ext}\,^e_R(M', R) \supseteq \mathrm{Ann}\,(M')$. But $\mathrm{Ann}\,(M') \supseteq \mathfrak{m}^n$ for some n, as M' is a finitely generated R-module of finite length. Therefore codimension of $I_e \geq e$.

2. By above Lemma, we have

$$I_e = \mathrm{Ann}\ \mathrm{Ext}\,^e_R(M', R) \subseteq \mathrm{Ann}\ \mathrm{Ext}\,^e_R(\mathrm{Ext}\,^e_R(M', R), R) \subseteq \mathrm{Ann}\,(M').$$

Therefore $I_e = \mathrm{Ann}\,(M')$. Now we need to prove that $\mathfrak{m} \in \mathrm{Ass}\,(M)$ if and only if $\mathfrak{m} \supseteq I_e$. Suppose $\mathfrak{m} \in \mathrm{Ass}\,(M)$ then $R/\mathfrak{m} \in M$. Therefore $M' \neq 0$ which implies $\mathrm{Ann}\,(M') \neq R$. Therefore $I_e = \mathrm{Ann}\,(M') \subseteq \mathfrak{m}$.

Conversely, if $\mathfrak{m} \supseteq I_e = \mathrm{Ann}\,(M')$. Then $\mathrm{Supp}\,(M') = \{\mathfrak{m}\}$, which implies $\mathrm{Ass}\,(M') = \{\mathfrak{m}\}$. Therefore $\mathfrak{m} \in \mathrm{Ass}\,(M') \subseteq \mathrm{Ass}\,(M)$.

3. Enough to prove that $(0 : I_e) = M'$; as we proved in statement 1 that the maximal ideal is not the associated prime of M/M' (here we recall that a prime ideal of height e is the maximal ideal after localization). Now since $\operatorname{Ann}(M') = I_e$ we have $M' \subseteq (0 : I_e)$. Let $x \in (0 : I_e)$ then $xI_e = 0$. If $\operatorname{codim} I_e > e$ then $I_e = R_e$, which implies that $x = 0$. If $\operatorname{codim} I_e = e$ then $\mathfrak{m}^n \subseteq I_e$, for some n, which implies $x \in M'$. This completes the proof of the theorem.

Corollory: For any $r \geq 0$, $\operatorname{Ass}(M) \cap \{\text{primes of height } r\} = \operatorname{Ass} \operatorname{hull}(I_r)$.

Proof: It follows from the above theorem and the definition of hull.

Lemma: Let N be a finite module over a Noetherian ring R. Then for every $\mathfrak{p} \in \operatorname{Ass}(\operatorname{Ann}(N))$ there exists $\mathfrak{q} \in \operatorname{Ass}(N)$ such that $\mathfrak{p} \subseteq \mathfrak{q}$.

Proof: As $\mathfrak{p} \in \operatorname{Ass}(\operatorname{Ann}(N))$, there exists $x \in A \setminus \operatorname{Ann}(N)$ such that $\operatorname{Ann}(x) = \mathbf{p}$ in $A/\operatorname{Ann}(N)$. Since $x \notin \operatorname{Ann}(N)$, there exists $n \in N$ such that $xn \neq 0$ in N. Therefore, one can choose $\mathbf{q} \in \operatorname{Ass}(N)$ such that $\mathbf{q} \supseteq \operatorname{Ann}(xn) \supseteq \mathbf{p}$.

Theorem: If $I \subseteq R$ is an ideal, where R is a regular domain then

$$\operatorname{hull}(I) = \operatorname{Ann}\ \operatorname{Ext}^c_R(R/I, R),$$

where $c = \operatorname{ht}(I)$.

Proof: By Corollary, every associated prime of $\operatorname{Ext}^c_R(R/I, R)$ is of codimension c. Therefore, by the above lemma, every associated prime of $\operatorname{Ann}\ \operatorname{Ext}^c_R(R/I, R)$ is of height $\leq c$. But $I \subseteq \operatorname{Ann}\ \operatorname{Ext}^c_R(R/I, R)$. Hence every associated prime of $\operatorname{Ann}\ \operatorname{Ext}^c_R(R/I, R)$ is of height c. Since associated primes of both the ideals are minimal of codimension c, to prove the equality it is enough to prove locally at primes of height c. So we can assume that R is a regular local ring of dimension c, with maximal ideal $\mathfrak{m}$. Now, by the claim of Theorem above,

$$\operatorname{Ann}\ \operatorname{Ext}^c_R(R/I, R) \simeq \operatorname{Ann}(H^0_{\mathfrak{m}}(S/I)) = \operatorname{Ann}(S/I) = I = \operatorname{hull}(I),$$

where the last equality follow from earlier Lemma. This proves the theorem.

Proposition: Let $\{x_1, \ldots, x_m\}$ be a regular sequence in an ideal I of codimension m of a regular ring R. Then

$$\operatorname{hull}(I) = ((x_1, \ldots, x_m) : ((x_1, \ldots, x_m) : I)).$$

Proof: By the above theorem, we have $\operatorname{hull}(I) = \operatorname{Ann}\ \operatorname{Ext}^m(R/I, R)$. Using Rees's formula for the first isomorphism below, we get

$$Ext^m(R/I, R) \xrightarrow{\sim} \operatorname{Hom}(R/I, R/(x_1, \ldots, x_m)) \xrightarrow{\sim} \frac{(((x_1, \ldots, x_m) : I))}{(x_1, \ldots, x_m)}$$

This proves the proposition.

Corollary: Let R be a regular ring, and let M be a finitely generated module. Let $\mathfrak{p}$ be a prime ideal of codimension r. The $\mathfrak{p} \in \operatorname{Ass}(M)$ if and only if it is a minimal prime of the support of $\operatorname{Ext}^r(M, R)$.

Proof: Support of $\operatorname{Ext}^r(M, R) = V(\operatorname{Ann}(\operatorname{Ext}^r(M)) = V(I_r)$. By above, I_r has codimension $\geq r$. We have also seen above that $I_r = \operatorname{Ann}(M')$ for some submodule M'

of M. Hence, $V(I_r) = V(\text{Ann}\,(M')) = \text{Supp}\ \ (M')$, and the minimal primes of I, are minimal primes of $\text{Supp}\,(M')$ and so belong to $\text{Ass}\,(M)$, since $M' \subseteq M$.

Corollary: The minimal primes of the ideal $J_r = \text{Ann}\ \ (\text{Ext}^{\,r}(\text{Ext}^{\,r}(M, R), R)$ are the associated primes of M of codimension r.

Proof: By the above Corollary, the associated primes of M of codimension r are the minimal primes of $\text{Ext}^{\,r}(M, R)$. Of course, the latter may have other associated primes, but all these will have codimension $> r$. Again apply above Corollary to the module $\text{Ext}^{\,r}(M, R)$. Therefore, minimal primes of $\text{Ext}^{\,r}(\text{Ext}^{\,r}(M, R), R)$ are the associated primes of $\text{Ext}^{\,r}(M, R)$ of codimension r, which are precisely the minimal primes of $\text{Ext}^{\,r}(M, R)$, and so are the associated primes of M of codimension r. Thus, taking "double Ext" has the effect of stripping off the "excess" unwanted additional associated primes acquired by $\text{Ext}^{\,r}(M, R)$.

Definition: The ideal $J_r = \text{Ann}\ \ (\text{Ext}^{\,r}(Ext^r(M, R), R))$ is called the *r-th equidimensional factor of M*. If $M = R/I$, then we denote J_r by $J_r(I)$.

Corollary: If I is an ideal of codimension m then

$$\text{Ass}\,(R/I) = \bigcup_{r \geq m} \text{Ass}\,(R/J_r(I)).$$

The above observation shows that the study of $Ass(R/I)$ is reduced to the study of $Ass(R/J_r(I))$. We study the ideals $J_r(I)$ a bit more below.

Proposition: Let R be a regular ring and let I be an ideal of codimension m. Then

- $J_r(I) = R$ for $0 \leq r \leq m$.
- $J_r(I)$ is either R or an equidimensional ideal of codimension r, viz, the intersection of the (unique) primary components of codimension r of $\text{Ann}\,((\text{Ext}^{\,r}(R/I, R))$.

Moreover, it is also the intersection of the primary components of codimension r of I. *(denoted by* $\text{hull}_{\,r}(I)$*)*

Proof: (i) Since I has codimension $m > r$, by earlier Proposition, we get that $\text{Ext}^{\,r}(R/I, R) = 0$. Therefore, $J_r(I) = R$.
(ii) If support $\text{Ext}^{\,r}(R/I, R)$ has codimension $\geq r$, then as in (i), $J_r(I) = R$.

Let $E = R/I$, E_0 be the submodule of E consisting of all elements whose support has codimension $> r$. Let $F = E/E_0$, then $\text{Ass}\,(F)$ has all primes of codimension r. Moreover, $\text{Ann}\,(F) = \text{hull}_{\,r}(I)$.

The exact sequence $0 \to E_0 \to E \to F \to 0$ induces the long exact sequence in cohomology

$$\text{Ext}^{\,r-1}_{\,R}(E_0, R) {\to} \text{Ext}^{\,r}_{\,R}(F, R) {\to} \text{Ext}^{\,r}_{\,R}(E, R) {\to} \text{Ext}^{\,r}_{\,R}(E_0, R)$$

By above Proposition, $\text{Ext}^{\,r-1}_{\,R}(E_0, R) = 0, \text{Ext}^{\,r}(E_0, R) = 0$, whence $\text{Ext}^{\,r}(F, R) \overset{\sim}{\to} \text{Ext}^{\,r}_{\,R}(E, R)$ Now $J_r(F) \overset{\sim}{\to} J_r(E)$, and so $\text{Ann}\, J_r(F) = \text{Ann}\ \ J_r(E)$. Hence, $J_r(I) = \text{Ann}\ \ J_r(E) = \text{Ann}\ \ J_r(F)$ is the intersection of the unique primary components of codimension r of $\text{Ann}\,(\text{Ext}^{\,r}(R/I, R)$.

On the other hand, we show that $\text{Ann}\,(F) = \text{Ann}\,(\text{Ext}^{\,r}_{\,R}(F, R))$! Let $a \in R$ which is regular on F. We have an exact sequence.

$$0 \to F \overset{a}{\to} F \to F/aF \to 0$$

The corresponding long exact sequence of cohomology is

$$\operatorname{Ext}^r_R(F/aF, R) \to \operatorname{Ext}^r_R(F.R) \xrightarrow{a} \operatorname{Ext}^r_R(F, R) \to \operatorname{Ext}^{r+1}_R(F, R)$$

Since a is regular on F, $\operatorname{Ext}^r(F/aF, R) = 0$. Hence, support of F/aF has codimension $\geq (r+1)$ by the previous Proposition. Hence, a is regular on $\operatorname{Ext}^r(F, R)$, as was required to be shown.

Finally, we give a method to compute the unique intersection of primary components of codimension equal to codimension of I. This is described via use of a regular sequence in I. (*Note.* In practice, it is not easy to find such a regular sequence of length codimension I.)

Proposition. Let $\{x_1, \dots, x_m\}$ be a regular sequence in an ideal I of codimension m of a regular ring. Then $\operatorname{hull}_m(I) = J_m(I) = (x_1, \dots, x_m) : ((x_1, \dots, x_m) : I)$

Proof. By Rees's formula,

$$\operatorname{Ext}^m(R/I, R) \tilde{\to} \operatorname{Hom}(R/I, R/(x_1, \dots, x_m)) \tilde{\to} \frac{(x_1, \dots, x_m) : I}{(x_1, \dots, x_m)}$$

(The last isomorphism is easy to see.)

Let I_0 be the intersection of the (unique) primary components of I of codimension m. As in proof of above Proposition, $\operatorname{Ext}^m_R(R/I_0, R) \tilde{\to} \operatorname{Ext}^m_R(R/I, R)$. ($F = R/I_0$ above !)

Hence, by Rees Lemma,

$$\operatorname{Ext}^m(R/I, R) \tilde{\to} \operatorname{Ext}^m(R/I_0, R) \tilde{\to} \frac{(\underline{x}) : I_0}{(\underline{x})},$$

where $\underline{x} = (x_1, \dots, x_m)$.

Now $J_r(I) = J_r(I_0) \supseteq \operatorname{Ann}(\operatorname{Ext}^m(R/I_0, R)) = (\underline{x}) : ((\underline{x}) : I_0)$.

For every minimal prime $\mathfrak{p} \supseteq J_r(I)$, we have $J_r(I)_\mathfrak{p} = J_r(I_0)_\mathfrak{p} = J_r((I_0)_\mathfrak{p}) = \mathfrak{q}_\mathfrak{p}$, where $\mathfrak{q}$ is the unique $\mathfrak{p}$-primary component of I_0. Also

$$(\operatorname{Ann}(\operatorname{Ext}^m(R/I_0, R))_\mathfrak{p} = \operatorname{Ann}(\operatorname{Ext}^m(R/I_0, R)_\mathfrak{p}) = \operatorname{Ann}(\operatorname{Ext}^m(R_\mathfrak{p}/(I_0)_\mathfrak{p}, R_\mathfrak{p})).$$

Note that $\operatorname{Ext}^m(R_\mathfrak{p}/(I_0)_\mathfrak{p}, R_\mathfrak{p})$ has codimension $\geq m$, and its annhilator contains $\operatorname{Ann}(R_\mathfrak{p}/(I_0)_\mathfrak{p}) = (I_0)_\mathfrak{p}$ Thus, $J_r(I)_p = \operatorname{Ann}(\operatorname{Ext}^m(R/I_O, R))_p$, for all minimal $p \supseteq J_r(I)$. Since both the ideal are equidimensional we can conclude that they are equal.

Finding the Associated Primes

We give a brief sketch of the ideas of Eisenbud-Huneke-Vasconcelos in [EHV] on how they would proceed to find the associated primes, and a primary decomposition of an ideal in a noetherian ring. No details or proofs are given here.

Suppose we want to find $\operatorname{Ass}(R/I)$:

1. First find the equidimensional components $I_m, I_{m+1}, \cdots$, etc. of I. These have been described in the last section in terms of certain "double Ext" modules, which we know can be computed.
   Hence, we will replace I by one of these, and proceed to find its associated primes. Hence, we can assume henceforth that I is an equidimensional ideal.
   Note moreover that all the associated primes of I are now embedded primes, hence one can determine the primary components, once one determines the associated primes. (This is done by residuation.)

2. Since we know how to compute $\sqrt{I}$ we may assume that I is a radical ideal. This will not affect the set $Ass(R/I)$.

3. We may add a fresh homogeneous variable and saturate, and assume that I is radical, equidimensional and homogeneous. (Justify!)

4. Now we have that R/I is a graded ring. Let A denote the integral closure. We shall sketch below how A can be computed effectively. (This is the hard part of the procedure, but its description is easy.) A is a finite product of integral domains. Hence, its minimal primes are in one-one correspondence with the idempotents of A.

   Moreover, the minimal primes of R/I are the intersection of the minimal primes of A with R/I. Hence, we need to only find the minimal primes of A. Equivalently, we need to find the idempotents of A.

5. Let E be a idempotent of A, i.e. $E^2 = E$. Hence, E must have degree zero! Thus, all the idempotents like in a *finite dimensional algebra* A_0! Moreover, the indecomposable idempotents of A_0 will generate the minimal prime ideals of A. We have already seen earlier that we can compute the idempotents of an artinian ring - hence we have a procedure to compute the idempotents of A_0!

6. Let us now describe how A, the integral closure of R/I looks: This has been done is several ways, say by G. Stolzenberg, A. Seidenberg, C. Traverso, etc. We give a recent description due to J.Brennan-W. Vasconcelos.

7. Choose a Noether normalization $T = k[x_1, \cdots, x_d] \subset R/I$. (We have already described earlier a procedure to get such a subring.)

8. Compute $A^{**} = \mathrm{Hom}_T(\mathrm{Hom}_T(R/I, T), T)$. It can be computed as follows: When we get the Noether normalization $T \subseteq R/I$, the process also yields a presentation of R/I: $T^p \xrightarrow{\varphi} T^q \to R/I \to 0$ The double dual of R/I is the module A^{**}.

   It can be shown that the module A^{**} is a subring of the integral closure A of R/I. *In fact, if R/I is regular in codimension one, then it will also be equal to A.* So the problem is easier in this situation. In the general situation, a lot more work needs to be done, which we only sketch very scantily below. (The less experienced reader should skip this part in the first reading or go to [V] where a few more details can be found.)

9. We replace R/I by A^{**}, which we now rename as B. A procedure has been given in [V] to obtain a presentation of B as a finitely generated k-algebra.

10. Let J be its Jacobian ideal. If the height of $(J) \geq 2$, then $B = A$. If the height of $(J) = 1$, then $C = \mathrm{Hom}\,(J^{-1}, J^{-1})$ is a subring of A which properly contains B. (Here J^{-1} denotes the fractional quotient ideal $(B : J)$ in the quotient field of B.) One replaces B by C, and continues the process above. Finally, it is shown that the height $(J) \geq 2$, and we will be through.

December 27,2002