

Commutative Algebra w/ Singular

Bernd Sturmfels

Nathan D. George

May 4, 2006

January 17

Note: We'll follow the text: *A Singular introduction to Commutative Algebra*

1 Rings, Ideals and standard bases

1.1 Rings, polynomials, and ring maps (1.1)

In this course, ring = A = commutative ring with identity. Some examples include: \mathbb{Z} , $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, any field. A polynomial ring looks like $k[x]$ or $k[x_1, \dots, x_n]$ over a field k , or $A[x_1, \dots, x_n]$ over a ring A . Monomials are given by $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ with a bijective correspondence to $\alpha \in \mathbb{N}^n$. We can establish a partial order where

$$"x^\alpha \text{ divides } x^\beta" \iff \alpha \leq_{\text{nat}} \beta$$

A term is a monomial times a coefficient $c \cdot x^\alpha$ with $c \in A \setminus \{0\}$, $\alpha \in \mathbb{N}^n$. Note that 0 is not a term nor a monomial. The (*total*) *degree* of a polynomial $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, a finite sum, is $\deg(f) = \max\{|\alpha| : c_\alpha \neq 0\}$.

See **Singular** for ring and polynomial declarations.

- $>$ is a global ordering if $x^\alpha > 1, \forall \alpha \neq 0$
- $>$ is a local ordering if $x^\alpha < 1, \forall \alpha \neq 0$
- $>$ is a mixed ordering otherwise

For the geometry, see Appendix A.

Lemma 1.1 (1.2.5). *For a monomial ordering, $>$, TFAE:*

1. $>$ is a well-ordering (every nonempty subset has a smallest element)
2. $x_i > 1 \forall i \in [n]$
3. $>$ is a global ordering

4. $>$ refines the divisibility ordering $\alpha \geq_{\text{nat}} \beta$ and $\alpha \neq \beta \implies x^\alpha > x^\beta$

Proof. (1) \implies (2) by contrapositive, so $\exists x_{i_0} < 1$, so $1 > x_{i_0} > x_{i_0}^2 > \dots$ has no smallest element.

(2) \implies (3) If we write $x^{\text{alpha}} = x^{\alpha'} \cdot x_i$, then use induction and apply assumption.

(3) \implies (4) If $\alpha - \beta \geq 0 \implies x^{\alpha-\beta} > 1$ by (3) which gives $x^\alpha > x^\beta$.

(4) \implies (1) by Dickson's Lemma, take a Dickson basis and take its minimal element. □

Now we'll define the monomial orderings, fix the 3 unknowns, $x > y > z$:
First we have the Global orderings:

1. Lexicographic: $1 < z < z^2 < \dots < y < yz < \dots < x < xz < \dots$
2. Degree: $1 < z < y < x < z^2 < yz < y^2 < xz \dots$
3. Degree Reverse Lex: $1 < x < y < x < z^2 < \dots$

Then we have the Local orderings:

1. Negative Lex: $1 > x > x^2 > \dots > y > xy > x^2y > \dots > z > xz > \dots$
2. Negative Degree Lex: $1 > x > y > z > x^2 > xy > y^2 > xz > yz > z^2 > \dots$
3. Negative Degree Reverse Lex: switch y^2 and xz above.

January 19

1.2 Ideals and Quotient Rings (1.3)

Definition 1.2. A subset $I \subset A$ is an *ideal* if $f, g \in I \implies f + g \in I$ (additive subgroup) and $f \in I, a \in A \implies af \in I$ (multiplicatively closed)

Generation: If $f_1, \dots, f_k \in A$, then

$$\begin{aligned} I &= \langle f_1, \dots, f_k \rangle \\ &= \text{ideal generated by } \{f_i\} \\ &= \text{smallest ideal containing } \{f_i\} \\ &= \{g_1 f_1 + \dots + g_k f_k \mid g_i \in A\} \end{aligned}$$

If $J \subset A$ (possibly infinite), we can write $\langle J \rangle = \{ \text{finite linear combinations} \}$.

If I and J are ideals, so are:

- $I + J = \text{ideal generated by } I \cup J$
- $I \cap J$
- $I \cdot J = \text{ideal generated by } \{f \cdot g \mid f \in I, g \in J\}$

Hilbert Basis theorem:

Definition 1.3. A commutative ring A is *Noetherian* if every ideal is finitely generated.

Theorem 1.4 (HBT (1890): (1.3.5)). *If A is a Noetherian ring, then $A[x_0, \dots, x_n]$ is also Noetherian.*

Proof. Note that by induction, it suffices to take $n = 1$: $A[x]$. $\exists I \subset A[x]$ ideal that is not finitely generated. Choose a sequence of polynomials as follows: \square

January 24

January 26

2 Rings associated to monomial orderings

Goal: compute efficiently in

$$K[x_1, \dots, x_n]_{\langle x_1, \dots, x_n \rangle}, l \leq n$$

Let \succ be a monomial ordering on $K[x] = K[x_1, \dots, x_n]$. The leading monomial function LM satisfies:

1. $LM(fg) = LM(f)LM(g)$
2. $LM(f + g) \leq \max\{LM(f), LM(g)\}$ with equality if leading terms don't cancel.

This implies $S_{\succ} = \{u \in K[x] - \{0\} \mid LM(u) = 1\}$ is multiplicatively closed. The ring associated to $(K[x], \langle \rangle)$ is

$$K[x]_{\succ} \equiv S_{\succ}^{-1}K[x] = \left\{ \frac{f}{u} \mid f, u \in K[x], LM(u) = 1 \right\}$$

Note:

$$S_{\succ} = K^* \iff \succ \text{ is global}$$

$$S_{\succ} = K[x] - \langle x_1, \dots, x_n \rangle \iff \succ \text{ is local}$$

Lemma 2.1. 1. $K[x] \subseteq K[x]_{\langle \rangle} \subseteq K[x]_{\langle x \rangle}$

2. Units: $(K[x]_{\succ})^* = \left\{ \frac{v}{u} \mid u, v \in K[x], LM(v) = LM(u) = 1 \right\}$

3. $K[x] = K[x]_{\succ} \iff \succ \text{ is global}$
 $K[x]_{\langle x \rangle} = K[x]_{\succ} \iff \succ \text{ is local}$

4. $K[x]_{\succ}$ is Noetherian and factorial

Example 2.2. $K[x, y] = K[\underbrace{x_1, \dots, x_n}_{>_1}, \underbrace{y_1, \dots, y_m}_{>_2}]$ and consider product orderings $\succ = (\succ_1, \succ_2)$

If $>_1$ is global, then $S_{>} = \{u \in K[y] \mid LM_{>_2}(u) = 1\}$ and hence $K[x, y]_{>} = (K[y]_{>_2})[x]$. This order has the *elimination property* $f \in K[x, y]$ and $LM(f) \in K[y] \Rightarrow f \in K[y]$.

Definition 2.3. (1.5.5) Leading data in $K[x]_{>}$. For $f \in K[x]_{>}$, choose $u \in K[x]$ such that $LT(u) = 1$ and $uf \in K[x]$. We define $LM(f) \equiv LM(uf)$, $LT(f) \equiv LT(uf)$, $LC(f) \equiv LC(uf)$, $LE(f) \equiv LE(uf)$, and $tail(f) \equiv f - LT(f)$. For any subset $G \subset K[x]_{>}$ define the *leading ideal*

$$L(G) = \langle LM(g) \mid g \in G - \{0\} \rangle_{K[x]}$$

Remark 2.4. These definitions are independent of the choice of u . Namely, since $K[x]_{>} \subset K[x]_{\langle x \rangle} \subset K[[x]]$. We may consider f as a formal power series and $LM(f)$ is its LM .

In other situations, like Lie algebras, given a ring you might have a two-sided ideal, but the leading ideal won't be in the ideal you started with, but a simpler ideal. This definition is just a taste in that direction.

Note: If I is an ideal the $L(I)$ is usually not generated by L (a generating set of I).

Example 2.5.

$$\begin{aligned} I &= \langle \underline{x} + y + z, \underline{x} - y + 2z \rangle \\ L(\text{gens}) &= \langle x \rangle \\ L(I) &= \langle x, y \rangle \end{aligned}$$

Example 2.6. Take $> = (\text{global}, \text{local})$ on $K[x, y]$, two variables.

$$f = \frac{2xy - x^2 + 5x}{3y + 7} \in K[x, y]_{>}$$

Quick reality check: What's $LM(f) = x^2$. Claim that if I take $u = 1 + \frac{7}{3}y$, then we satisfy $uf = 1$. Let's change the ordering to take "ds" ordering. Then $LT(f) = \frac{5}{7}x$, $LE(f) = (1, 0)$.

Now look at ring maps between rings associated to $>$:

Lemma 2.7. (1.5.8) Let $\psi : K \rightarrow L$ be a field homomorphism, and $>_1, >_2$ monomial orderings on $Mon(x_1, \dots, x_n)$ and $Mon(y_1, \dots, y_m)$. Let $f_1, \dots, f_n \in L[y_1, \dots, y_m]_{>_2}$ and assume that

$$h \in S_{>_1} \Rightarrow h(f_1, \dots, f_n) \in S_{>_2} \quad (*)$$

Then there exists a unique ring map

$$\phi : K[x]_{>_1} \rightarrow L[y]_{>_2}$$

satisfying $\phi(x_i) = f_i$ for $1, \dots, n$ and $\phi(a) = \psi(a)$ for $a \in K$.

Proof. By Lemma (1.1.6), $\exists!$ ring map $\tilde{\phi} : K[x] \rightarrow L[y]_{>_2}$ with $\tilde{\phi}(x_i) = f_i$ and $\tilde{\phi}(a) = \psi(a)$ for $a \in K$. (*) says that $\tilde{\phi}(u)$ is a unit in $L[y]_{>_2}$ for each $u \in S_{>_1}$. The Universal property of localization (Prop 1.4.7) implies the result. \square

Special case: $K = L$, $>_1$ global, (*) is void. $K[x] \rightarrow K[y]_{>}$ is specified by $f_1, \dots, f_m \in K[y]$. Now to Singular.

```

> int n,m=2,3;
> ring A1=0,(x(1..n),y(1..m)),(dp(n),ds(m));
> ring A2=0,(x(1..n),y(1..m)),(ds(n),dp(m));

```

What type of rings are these? Let's try writing it in set notation:

$$\left\{ \begin{array}{l} f(x,y) \\ g(x,y) \end{array} \mid g(x,y) = \dots \right\}$$

Draw $\text{Spec}(A2)$

January 31

3 Normal forms and standard bases

GS1: Jason Morton, Office hours, T/H 10:30-12 @ 1040 Evans. email: mortonj@math.berkeley.edu

$R = K[x_1, \dots, x_n]_{>}$, with $>$ a monomial ordering.

Definition 3.1. If $I \subset R$ is an ideal, then a finite subset $\mathcal{G} \subset I$ is a *standard basis* if $L(I) = L(\mathcal{G})$. If $>$ is a global ordering, then \mathcal{G} is a *Gröbner basis*.

Remark 3.2. Every non-zero ideal I has a standard basis (Dickson's Lemma).

Generalizes the Euclidean algorithm (for $n = 1$) and Gaussian elimination (for linear polynomials).

Definition 3.3. A set $G \subset R$ is *interreduced* if $LM(g) \not\mid LM(f)$ for $f \neq g$ in G . $f \in R$ is *reduced* with respect to G if no monomial in the power series expansion of f lies in $L(G)$. Finally, $G \subset R$ is (*completely*) *reduced* if

- G is interreduced, and
- for any $g \in G$: $LC(g) = 1$ and $tail(g)$ is reduced with respect to G .

If $>$ is global, then every I has a unique reduced Gröbner basis.

Other useful programs include Maple, Mathematica, Magma, M2.

Note: If $n = 1$ and $G = \{x - x^2\}$ with local ordering. Then G is interreduced but not reduced. $I = \langle G \rangle = \langle x \rangle \in R$.

Definition 3.4. (1.6.4) Let \mathcal{G} be the set of all finite lists G in R . A map

$$\begin{aligned} NF : R \times \mathcal{G} &\rightarrow R \\ (f|G) &\mapsto NF(f|G) \end{aligned}$$

is a *normal form* on R if

1. $NF(0|G)=0$
2. $NF(f|G) \neq 0 \implies LM(NF(f|G)) \notin L(G)$
3. If $G = [g_1, \dots, g_s]$, then $r = f - NF(f|G)$ has a *standard representation*: Either $r = 0$ or $r = a_1g_1 + a_2g_2 + \dots + a_sg_s$ with $a_i \in R$ satisfying $LM(f) \geq LM(a_i g_i) \forall i$ with $a_i g_i \neq 0$

If $\forall f \in R, \forall g \in G : NF(f|G)$ is reduced with respect to G , then NF is a *reduced normal form*.
 A map $NF : R \times G \rightarrow R$ is a *weak normal form* if it satisfies (1) and (2) and

- 2'. $\forall f \in R \forall G \in \mathcal{G} \exists \text{ unit } u \in R^* : uf - NF(\underbrace{\quad}_u f|G)$ has a standard representation w.r.t. G
 ? : book typo

If u can be chosen in $R^* \cap K[x]$, then NF is a *polynomial weak normal form*

Example 3.5. $G = [(y-x)(1-y)]$ ds $I = \langle y-x \rangle$ $f = y$ has no polynomial normal form but $h = x(1-y)$ is a polynomial weak NF with $u = 1-y$.

Lemma 3.6. (1.6.7) *Let $I \subset R$ be an ideal and $G \subset I$ a standard basis of I and $NF(\cdot|G)$ a weak normal form*

1. For any $f \in R$ we have $(f \in I \iff NF(f|G) = 0)$
2. If $J \subset R$ is an ideal with $I \subseteq J$, then $(L(I) = L(J) \implies I = J)$
3. $I = \langle G \rangle_R$, that is, the standard basis generates I as an R -ideal.
4. If $NF(\cdot|G)$ is a reduced normal form then it is unique

Proof. 1. If $NF(f|G) = 0$, then $uf \in I$ and hence $f \in I$. If $NF(f|G) \neq 0$, then $LM(NF(f|G)) \notin L(G) = L(I) \implies f \notin I$ since $\langle G \rangle_R \subseteq I$

2. Let $f \in J$ and assume $NF(f|G) \neq 0 \implies LM(NF(f|G)) \notin L(G) = L(I) = L(J)$ contradicting $NF(f|G) \in J$

The rest are similar. □

If $f, g \in R \setminus \{0\}$ with $LM(f) = x^\alpha, LM(g) = x^\beta$, set $x^\gamma = lcm(x^\alpha, x^\beta)$. The *s-polynomial* of f and g is

$$spoly(f, g) = x^{\gamma-\alpha} \cdot f - \frac{LC(f)}{LC(g)} x^{\gamma-\beta} \cdot g$$

For the rest of today, assume that $>$ is global.

Algorithm 3.7. (1.6.10) (NF Buchberger ($f|G$))

Input: $f \in K[\bar{x}], G \in \mathcal{G}$.

Output: $h \in K[x]$, a normal form of f w.r.t. G

```
> h:=f
> while (h != 0) &
```

$G_h := \{g \in G : LM(g)|LM(h)\} \neq \emptyset$, choose any $g \in G_h$,

```
h:=spoly(h,g)
```

(we have here $\gamma = \alpha$)

```
> return h
```

Q: Why does this terminate?

A: Because $>$ is a global ordering

Algorithm 3.8. (1.6.11) (Red NF Buchberger ($f|G$))

```
> h:=0, g:=f
> while (g != 0)
  g:= NF Buchberger (g|G)
  if(g != 0)
    h:= h + LT(g)
    g:= tail(g)
> return
```

Example 3.9. $x > y > z$, dp , $G = \{x, y\}$, $f = x^3 + y^2 + 2z^2 + x + y + 1$

$$\begin{aligned} NF\text{Buchb}(f|G) &= 2z^2 + x + y + 1 \\ RedNF\text{Buchb}(f|G) &= z^2 + \frac{1}{2} \end{aligned}$$

Example 3.10. Discriminant Example:

```
> ring R=0,(x,y,z,e1,e2,e3),lp;
> poly d = (x-y)^2*(x-z)^2*(y-z)^2;
> d;
  x^4*y^2-2*x^4*y*z+x^4*z^2-2*x^3*y^3+ (19 terms)
> ideal I=x+y+z-e1, x*y+x*z+y*z-e2,..., x*y*z-e3;
> reduce(d,I);
  4*y^6+12*y^5*z-12*y^5*e1-3*y^4*z^2-18*y^4*z*e1+...
> ideal G = std(I); G:
G[1]=z^3-z^2*e1+z*e2-e3 G[2]=y^2+y*z-y*e1+z^2-z*e1+e2 G[3]=x+y+z-e1
>reduce(d,G);
```

More to come in section 1.8.11, page 85, Subalgebra Membership

February 7

4 Operations on ideals and their computation (1.8)

4.1 Elimination of variables (1.8.2)

Given an ideal $I = \langle f_1, \dots, f_k \rangle \subset K[x]$ and $s < n$, find generators for the ideal $I' = I \cap K[x_{s+1}, \dots, x_n]$.

Solution: Use an elimination ordering, e.g. $(dp(s), dp(n-s))$ and compute a Gröbner basis G for I . Then $G \cap K[x_{s+1}, \dots, x_n]$ is a Gröbner basis for $I \cap K[x_{s+1}, \dots, x_n]$.

Geometric interpretation: The $\mathcal{V}(I') \subset K^s$ is the *Zariski closure* of the image of the variety $\mathcal{V}(I) \subset K^s$ under the coordinate projection

$$K^n \rightarrow K^s, \text{ with } (u_1, \dots, u_n) \mapsto (u_{s+1}, \dots, u_n)$$

. If $K = \mathbb{C}$ then Zariski closure here agrees with strong closure.

For a good but easy introduction into Algebraic Geometry, see Mumford's 'Red Book' available online (for free?) with the Springer lecture notes.

Example 4.1. ($n = 2, s = 1$)

$$I = \langle \underline{x}^2 - y^2 - 1, \underline{x} + y - \frac{1}{2} \rangle \text{ and } I' = \langle 8y^2 - 4y - 3 \rangle$$

$$\mathcal{V}(I) = \{(-0.41, 0.91), (0.91, -0.41)\}, \text{ and } \mathcal{V}(I') = \{-0.41, 0.91\}$$

4.2 Zariski closure of the image (1.8.3)

Given a ring map

$$\phi : K[x_1, \dots, x_n] \rightarrow K[t_1, \dots, t_m], \quad x_i \mapsto f_i(t)$$

and an ideal $\langle (g_1(t), \dots, g_s(t)) \rangle = I \subset K[t_1, \dots, t_m]$, we wish to compute the ideal $\phi^{-1}(I)$ in $K[x]$.

Geometric interpretation: $\mathcal{V}(\phi^{-1}(I)) \subset K^n$ is the Zariski closure of the image of $\mathcal{V}(I) \subset K^m$ under the induced map $\phi^* : K^m \rightarrow K^n$.

Solution: Form the ideal of the graph of ϕ^* . If you know how to do coordinate projections, then you can calculate arbitrary images.

$$\langle (g_1(t), \dots, g_s(t), x_1 - f_1(t), \dots, x_n - f_n(t)) \rangle \text{ in } K[t_1, \dots, t_s, x_1, \dots, x_n]$$

and eliminate t_1, \dots, t_s . This is often used with $I = 0$, (so there are no g 's at all), to compute the (Zariski closure of the) image of a map $\phi^* : K^m \rightarrow K^n$. We leave off the parenthetical part to imply calculating an image always means the Zariski closure of the image.

Example 4.2. Determine the unique algebraic relation among the power ring ($m = 2, n = 3$)

$$p_2 = t_1^2 + t_2^2, p_3 = t_1^3 + t_2^3, p_4 = t_1^4 + t_2^4$$

i.e. compute the kernel of

$$\mathbb{Q}[p_2, p_3, p_4] \rightarrow \mathbb{Q}[t_1, t_2], \quad p_i \mapsto t_1^i + t_2^i$$

i.e. compute the image of the map

$$\mathbb{C}^2 \rightarrow \mathbb{C}^3, \quad t \mapsto (p_2(t), p_3(t), p_4(t))$$

Answer: $p_2^6 - 4p_2^3p_3^2 - 4p_3^4 + 12p_2p_3^2p_4 - 3p_2^2p_4^2 - 2p_4^3$.

Book: p72-73. Maps between spectra of local rings.

4.3 Radical Membership (1.8.6)

Given an ideal $I = \langle f_1, \dots, f_k \rangle \subset K[\bar{x}]$ and $f \in K[\bar{x}]$ decide whether $f \in \sqrt{I}$?

Solution: Add a new variable t and form the ideal $J = \langle f_1(x), \dots, f_k(x), 1 - t \cdot f(x) \rangle \in K[\bar{x}][t]$. Then $1 \in J \iff f \in \sqrt{I}$. This proved in Lemma 1.8.8.

Aside: Compute \sqrt{I} from I is much harder.

4.4 Intersection of Ideals (1.8.7)

Given $I_1 = \langle f_1, \dots, f_s \rangle$ and $I_2 = \langle g_1, \dots, g_r \rangle$ in $K[\bar{x}]$, how do we compute generators for $I_1 \cap I_2$?

Solution: Add a new variable t and form the ideal

$$J = \langle tf_1(x), \dots, tf_s(x), (1-t)g_1(x), \dots, (1-t)g_r(x) \rangle \in K[\bar{x}, t].$$

Then $J \cap K[\bar{x}] = I_1 \cap I_2$ so just eliminate t . (Lemma 1.8.10)

Application: Interpolation (Intersection of maximal ideal). To illustrate, take the four points in the plane: $(1, 1), (1, 3), (3, 5), (4, 2)$. Then our ideal would be

$$\langle x-1, y-1 \rangle \cap \langle x-1, y-3 \rangle \cap \langle x-3, y-5 \rangle \cap \langle x-4, y-2 \rangle \subset \mathbb{Q}[x, y]$$

Now under a lexicographical Gröbner basis, this becomes:

$$\langle y^4 - 11y^3 + 41y^2 - 61y + 30, x - \frac{13}{12}y^3 + \frac{19}{2}y^2 - \frac{288}{12}y + \frac{19}{2} \rangle$$

4.5 Quotients of Ideals (1.8.8)

Give $I_1 = \langle f_1, \dots, f_s \rangle$ and $I_2 = \langle g_1, \dots, g_r \rangle \in K[\bar{x}]$, how do we compute $(I_1 : I_2) = \{h \in K[\bar{x}] | hI_2 \subseteq I_1\}$, sometimes referred to as the *colon* ideal, which can also be written as

$$(I_1 : \langle g_1 \rangle) \cap (I_1 : \langle g_2 \rangle) \cap \dots \cap (I_1 : \langle g_r \rangle)?$$

So it suffices to compute $I_1 : \langle g_i \rangle$.

Solution: Compute $I_1 \cap \langle g_i \rangle = \langle g_i h_1, g_i h_2, \dots, g_i h_t \rangle$. We don't want to 'factor' polynomials, but just remove factors. Thus we divide each generator by g_i to get $(I_1 : \langle g_i \rangle) = \langle h_1, h_2, \dots, h_t \rangle$ (lemma 1.8.12)

4.6 Saturation (1.8.9)

Compute the quotient of I_1 by successive powers of I_2 :

$$I_1 \subset (I_1 : I_2) \subset (I_1 : I_2^2) \subset (I_1 : I_2^3) \subset \dots$$

This becomes stationary, so

$$\exists s : (I_1 : I_2^s) = I_1 : I_2^{s+1} = (I_1 : I_2^\infty)$$

This is the *saturation* of I_1 with respect to I_2 .

Geometric Interpretation:

$$\mathcal{V}((I_1 : I_2^\infty)) = \overline{\mathcal{V}(I_1) \setminus \mathcal{V}(I_2)}$$

For example, $I_1 = \langle x^5 y^7 \rangle$, $I_2 = \langle y^2 \rangle$ gives $(I_1 : I_2) = \langle x^5 y^5 \rangle$, $(I_1 : I_2^2) = \langle x^5 y^3 \rangle$, $(I_1 : I_2^\infty) = \langle x^5 \rangle$.

Thursday Bring your friend. Solving polynomial equations. Read sections 1.8.4 and 1.8.5, pp74-77.

4.7 Subalgebra Membership (1.8.15)

Is f in $K[f_1, \dots, f_k] \subset K[\bar{x}]$?

Solution: Compute a Gröbner basis G of

$$\langle y_1 - f_1(x), y_2 - f_2(x), \dots, y_k - f_k(x) \rangle$$

with respect to an elimination ordering $x > y$ and check whether the normal form of $f(x)$ with respect to G contains no x_i , i.e. $\text{NF}_G(f(x)) = h(y_1, \dots, y_k)$

February 9

All the notes for today's lecture come from the handout, which is a copy of pp13-27 of Sturmfels' book.

5 SSPE, Gröbner Bases of 0 dimensional Ideals

$I = \langle f_1, \dots, f_m \rangle \subset \mathbb{Q}[\bar{x}]$, $\mathcal{V}(I) \subset \mathbb{C}^n$ its variety, $<$ a global ordering.

$$\begin{aligned} \mathcal{B} = \mathcal{B}_{<}(I) &= \{\text{monomials } x^A \notin \text{in}_{<}(I), L(I)\} \\ &= \text{the set of } \textit{standard monomials}. \end{aligned}$$

Proposition 5.1 (Fund Theorem of Algebra (2.1)). $\mathcal{V}(I)$ is finite $\iff \mathcal{B}$ is finite, and the cardinality of \mathcal{B} equals the cardinality of $\mathcal{V}(I)$ counting multiplicities.

Example 5.2. ($n = m = 3$)

$$I = \langle (x - y)^3 - z^2, (z - x)^3 - y^2, (y - z)^3 - x^2 \rangle$$

with ordering $> \text{dp}$.

$$\in_{<}(I) = \langle \underline{x}^3, x^2y, x^2z, xy^2, xyz^2, xz^3, \underline{y}^3, y^2z, yz^3, \underline{z}^4 \rangle$$

$$\mathcal{B} = \{1, x, x^2, xy, xyz, xz, xz^2, y, y^2, yz, yz^2, z, z^2, z^3\}$$

gives 14 roots counting multiplicities.

Note: \mathcal{B} is a \mathbb{Q} -basis for the vector space $\mathbb{Q}[x]/I$.

Theorem 5.3 (2.2). A zero-dimensional I is radical \iff the n elimination ideals $\text{In}\mathbb{Q}[x_i] = \langle p_i(x_i) \rangle$ are all radical. Otherwise,

$$\text{Rad}(I) = I + \langle p_{1,\text{red}}, p_{2,\text{red}}, \dots, p_{n,\text{red}} \rangle$$

where $p_{i,\text{red}}(x_i) = p_i(x_i) / \text{gcd}(p_i(x_i), p'_i(x_i))$.

In our example,

$$\text{In } \mathbb{Q}[x] = \langle \underbrace{x^8 + \frac{6}{25}x^6 + \frac{17}{625}x^4 + \frac{8}{15625}x^2}_{p(x)} \rangle$$

with $p_{\text{red}}(x) = p(x)/x$.

$$\text{Rad}(I) = I + \langle p_{\text{red}}(x), p_{\text{red}}(y), p_{\text{red}}(z) \rangle$$

has seven distinct roots: $(0, 0, 0) \leftarrow$ multiplicity 8 and six complex roots. (See Prop 2.5 and p17 top of handout)

If you go to your friend and ask him to tell you the roots and then he tells you with his computer that a root is $(0, 0, 0)$, then you do this next part to get the non-trivial roots.

$$\left(I : \underbrace{\langle x, y, z \rangle^\infty} \right) = ?$$

The companion matrix for the polynomial $x^3 + ax^2 + bx + c$ is:

$$\det \begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix} - k \cdot I$$

and $\mathbb{Q}[x]$ modulo this polynomial is $\simeq \mathbb{Q}[T]$.

5.1 Companion matrices (2.3)

I is a 0-dimensional ideal in $S = \mathbb{Q}[x]$, with a known Gröbner basis. The set \mathcal{B} of standard monomials is a basis for $S/I \simeq \mathbb{Q}^d$. Multiplication by a variable defines an endomorphism, $T_i : S/I \rightarrow S/I$, $f \mapsto x_i f$. We represent T_i by a $d \times d$ -matrix with rows and columns indexed by \mathcal{B} . If $x^u, x^v \in \mathcal{B}$, the entry of T_i in row x^u and column x^v is the coefficient of x^u in the normal form of $x^v x$.

Note: $T_i T_j = T_j T_i$ and $\mathbb{Q}[T_1, \dots, T_n] \simeq S/I$, $T_i \mapsto x_i$.

Theorem 5.4 (Stickelberger's Theorem). *The complex zeros are the joint eigenvalues:*

$$\mathcal{V}(I) = \{ (\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n \mid \exists v \in \mathbb{C}^d \setminus \{0\} \forall i, T_i v = \lambda_i v \}$$

Proof. ' \supseteq ' Suppose $v \in \mathbb{C}^d \setminus \{0\}$ with $T_i v = \lambda_i v \forall i \Rightarrow$ For any polynomial $p \in S : p(T_1, \dots, T_n) \cdot v = p(\lambda_1, \dots, \lambda_n)v$. If $p \in I$, then $p(T_1, \dots, T_n)$ is the zero matrix, hence $p(\lambda_1, \dots, \lambda_n) = 0 \Rightarrow (\lambda_1, \dots, \lambda_n) \in \mathcal{V}(I)$.

' \subseteq ' (assuming I is radical) Let $\lambda \in \mathcal{V}(I) \subset \mathbb{C}^n$. I claim \exists polynomial $q \in S \otimes_{\mathbb{Q}} \mathbb{C}$ such that $q(\lambda) = 1, q \equiv 0$ on $\mathcal{V}(I) \setminus \{\lambda\}$. This implies $x_i q(x) = \lambda_i q(x)$ on $\mathcal{V}(I)$. Therefore,

$$(x_i - \lambda_i)q \underbrace{\in}_{\text{Nullstellensatz}} \text{Rad}(I) = I$$

Let v be the image of q in $S/I \otimes \mathbb{C} \simeq \mathbb{C}^d$, then v is a joint eigenvector of (T_1, \dots, T_n) with eigenvalues $(\lambda_1, \dots, \lambda_n)$. \square

Corollary 5.5 (2.7). *The companion matrices T_1, \dots, T_n can be simultaneously diagonalized $\iff I$ is a radical ideal.*

5.2 Trace form (Real roots) (2.4)

Fix any polynomial $h \in S$ and consider the bilinear form $B_h : S/I \times S/I \rightarrow \mathbb{Q}$, with $(f, g) \mapsto \text{trace}((fgh)(T_1, \dots, T_n))$. We represent this bilinear form B_h by a symmetric $d \times D$ -matrix over \mathbb{Q} with respect to \mathcal{B} . The entry of B_h in row x^u and column x^v is the sum over $x^w \in B$ of (the coefficient of x^w in the normal form of $x^{u+v+w}h$).

The *signature* of B_h is the number of positive eigenvalues of B_h minus the number of negative eigenvalues.

Theorem 5.6 (2.8). *The signature of the trace form B_h equals the number (not counting multiplicities) of real roots $p \in \mathbb{R}$ of I with $h(p) > 0$ minus the number of real roots p of I with $h(p) < 0$.*

Corollary 5.7 (2.9). *The number of real roots of I equals the signature of B_1 .*

Example 5.8 ($n=1$).

$$I = \langle x^3 - a_2x^2 - a_1x - a_0 \rangle$$

$$B_1 = \begin{pmatrix} \beta_0 & \beta_1 & \beta_2 \\ \beta_1 & \beta_2 & \beta_3 \\ \beta_2 & \beta_3 & \beta_4 \end{pmatrix}$$

with $\beta_i = \sum_{j=0}^2 \text{coeff}_{x^j}(nf_I(x^{i+j}))$, and $nf_I(x^4) = (a_1 + a_2^2)x^2 + (a_0 + a_1a_2)x + a_0a_2$.

5.3 Solving equations in Singular (2.5)

Here's an open problem that Sturmfels would be oh so happy if we solved.

Mathieu's Problem: Does there exist a Laurent polynomial

$$f(x) = x^{-n} + a_{n-1}x^{-n+1} + \dots + a_1x^{-1} + x^n + b_{n-1}x^{n-1} + \dots + b_1x^1$$

with complex coefficients all of whose powers have zero constant term?

Now let's phrase the problem in terms of ideals: For $i \geq 2$, let $[f_i]$ denote the constant term of f^i , and consider

$$I = \langle [f^2], [f^3], \dots \rangle \subset \mathbb{Q}[a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1}]$$

Mathieu Is $\mathcal{V}(I) = \emptyset$? \iff Is $I = \langle 1 \rangle$? Yes (ask for paper) but:

Open problems:

- Is $\langle [f^2], [f^3], \dots, [f^{2n-1}] \rangle = \langle 1 \rangle$?
- How many complex solutions over $\langle [f^2], [f^3], \dots, [f^{2n-2}] \rangle$ have?

Look at exercise 13 in the handout.

February 14

. How do we compute $\ker(\varphi), \text{im}(\varphi), \text{coker}(\varphi)$? If the determinant is ± 1 , then you can do row and column operations to eliminate. But the determinant is 6 and there's only abstract abelian group of order 6. So under a change of basis we can get either a matrix with $\text{diag}(2,3,1)$ or $\text{diag}(6,1,1)$ which are supposedly isomorphic.

Proposition 6.6 (2.1.16). *Let $\varphi : M \rightarrow N$ an A -module homomorphism, then $\text{im}(\varphi) \simeq M / \ker(\varphi)$*

Corollary 6.7 (2.1.17). *Let $L \supset M \supset N$ be A -modules. Then $(L/N)/(M/N) \simeq L/M$.*

Proof. (2.1.16 \Rightarrow 2.1.17) The inclusion $N \subset M$ induces a homomorphism $\pi : L/N \rightarrow L/M$ of A -modules. We have π is surjective and $\ker(\pi)$ is M/N . \square

Question: How to tell whether a given submodule of $K[x, y]^n$ is free? e.g.

$$\begin{pmatrix} x^2 \\ xy \\ y^2 \end{pmatrix} \text{ and } \begin{pmatrix} xy \\ y^2 \end{pmatrix}$$

is not free.

Consider

$$\varphi : \mathbb{Q}[x, y]^4 \xrightarrow{[xy^5, x^2y^3, x^3y^2, x^5y]} \mathbb{Q}[x, y]$$

What's the $\text{im}(\varphi), \ker(\varphi), \text{coker}(\varphi)$? Well the image is the monomial ideal. Draw a graph in the x-y plane with the exponents as coordinates, then you draw a 'staircase' connecting the dots and shade the ideal as that above the stair. Below the stair are the standard monomials which form the cokernel. The number of standard monomials is the number of solutions. There are 4 choose 2 (=6) s-pairs of vectors in the kernel. They can be pictorially represented by linking the dots where they intersect in the graph and the change in x and y to get to that linking point.

February 16

Proposition 6.8 (2.1.21). *Let M be an A -module and $N_1, N_2 \subset M$ are submodules. Then*

$$(N_1 + N_2)/N_1 \simeq N_2/(N_1 \cap N_2)$$

Proof. The inclusion $N_2 \subset N_1 + N_2$ induces a surjective (why?) homomorphism $\pi : N_2 \rightarrow (N_1 + N_2)/N_1$ with $\ker(\pi) = N_1 \cap N_2$. Now use Proposition 2.1.15 \square

An A -module M is *finitely generated* if $M \simeq A^n/L$ for some $n \in \mathbb{N}$ and a submodule L . Equivalently, \exists a surjective A -linear map $A^n \rightarrow M$. An A -module is *finitely presented* if there exists an $n \times m$ -matrix φ such that M is the cokernel of $A^m \xrightarrow{\varphi} A^n$. We write

$$A^m \xrightarrow{\varphi} A^n \twoheadrightarrow M$$

to denote the presentation.

Question: What's the relationship between these two? In general, $fp \not\stackrel{\Rightarrow}{=} fg$.

Definition 6.9. An A -module M is *Noetherian* if every submodule N of M is finitely generated.

Lemma 6.10 (2.1.28). 1. Submodules and quotients of Noetherian modules are Noetherian.

2. If $N \subset M$ are A -modules, then M is Noetherian \iff both N and M/N are.

3. For an A -module M , TFAE:

(a) M is Noetherian

(b) Every ascending chain of submodules becomes stationary

(c) Every non-empty set of submodules of M has a maximal element (with respect to inclusion)

Proposition 6.11 (2.1.29). Let A be a Noetherian ring and M a finitely generated A -module, then M is a Noetherian A -module. (In particular, 'fp \iff fg' over a Noetherian ring)

Proof. Using Lemma 2.1.28, we may assume $M = A^n$. For $n = 1$, we're good. For $n \geq 2$: Consider $\pi : A^n \rightarrow A^{n-1}$. We have $A^{n-1} = A^n / \ker(\pi)$ and $\ker(\pi) = \{(0, \dots, 0, a) \in A^n \mid a \in A\} \simeq A$. Use Lemma 2.1.28 (2). \square

Lemma 6.12 (2.1.9). The sum of submodules of an A -module, the product of an ideal with an A -module, the direct sum and the direct product of A -modules are all A -modules.

The *module quotient* (but we'll call this the *colon module*) of two submodules M_1, M_2 of an A -module is an ideal in A

$$M_1 : M_2 = \{a \in A \mid aM_2 \subseteq M_1\}$$

The *annihilator* of M_2 is

$$\langle 0 \rangle : M_2$$

The quotient of a submodule by an ideal is a submodule of M .

$$M_1 : I = \{m \in M \mid I \cdot m \subseteq M_1\}$$

The *torsion module* is a submodule of M .

$$\text{Tors}(M) = \{m \in M \mid \exists \text{ non-zero-divisor } a \in A \text{ such that } a \cdot m = 0\}$$

If $\text{Tors}(M) = 0$, then M is *torsion-free*.

If $\text{Tors}(M) = M$ then M is a *torsion module*.

Example 6.13. $A = \mathbb{Q}[x, y]$ cyclic, $M = \mathbb{Q}[x, y] / \langle x^5 - y^5, x^7 - y^7 \rangle$. What is $\text{Tors}(M)$? M

Singular Example 2.1.20:

```
> ring A = 0, (x,y,z), (c,dp);
> module M=[xy,xz], [x,x];
> module N=[y2,z2], [x,x];
> M+N;
_[1]=[xy,xz] _[2]=[y2,z2] _[3]=[x,x]
> intersect(M,N);
_[1]=[x,x] _[2]=[xy2,xz2]
> quotient(M,N);
```

```

_[1]=x
> quotient(N,M);
_[1]=y+z
> qring Q=std(x5);
> module M=fetch(A,M);

```

Lemma 6.14 (Nakayama's Lemma 2.1.30). *Let A be a ring and $I \subset A$ an ideal which is contained in the Jacobson radical of A (= intersection of all maximal ideals). Let M be a finitely generated A -module and $N \subset M$ a submodule such that $M = IM + N$. Then $M = N$. In particular, if $M = IM$, then $M = 0$.*

Over a local ring, it's true for any ideal. Over a polynomial ring, it's true for no ideal.

Proof. By passing to the quotient module, it suffices to consider the case $N = \langle 0 \rangle$. Assume $M \neq \langle 0 \rangle$ and let $\{m_1, \dots, m_n\}$ be a minimal set of generators of M . Since $m_n \in M = IM$ we can choose ideal elements $a_1, \dots, a_n \in I$ such that $m_n = \sum_{i=1}^n a_i m_i$. This implies that $(1 - a_n)m_n = \sum_{i=1}^{n-1} a_i m_i$. By exercise 1.4.4, $1 - a_n$ is a unit in A . Therefore, m_1, \dots, m_{n-1} generate M . \square

Corollary 6.15 (2.1.31). *Let (A, \underline{m}) be a local ring and let M be a finitely generated A -module. Let's pick elements in the module $m_1, \dots, m_n \in M$ whose classes generate the A/\underline{m} -vector space $M/\underline{m}M$. Then m_1, \dots, m_n generate M .*

Proof. Let $N = Am_1 + \dots + Am_n$ and consider the following map

$$N \xrightarrow{\psi} M \xrightarrow{\varphi} M/\underline{m}M$$

Since the composition $\varphi \circ \psi$ is surjective, $N + \underline{m}M = M$. Now we use the Lemma 2.1.30. \square

Note: $\{m_1, \dots, m_n\}$ is a minimal set of generators \iff their classes form a basis of a vector space $M/\underline{m}M$. In this case, $n = \dim_{A/\underline{m}}(M/\underline{m}M)$.

Example 6.16. $A = \mathbb{Q}[x, y, z]_{\langle x, y, z \rangle}$. How many elements are needed to generate the module

$$\begin{aligned}
M_1 &= \ker(A^3 \xrightarrow{\begin{pmatrix} x & y & z \end{pmatrix}} A^1) \\
M_2 &= \ker(A^3 \xrightarrow{\begin{pmatrix} x-1 & y-1 & z-1 \end{pmatrix}} A^1)
\end{aligned}$$

So clearly, $A/\underline{m} = \mathbb{Q}$, so we have

$$\dim(M_1/\underline{m}M_1 = \ker(\mathbb{Q}^3 \xrightarrow{\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}} \mathbb{Q})) = 3$$

and

$$\dim(M_2/\underline{m}M_2 = \ker(\mathbb{Q}^3 \xrightarrow{\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}} \mathbb{Q})) = 2$$

So we only need 2 elements to generate M_2 . Claim that the following two vectors generate M_2

$$\begin{pmatrix} y-1 \\ 1-x \\ 0 \end{pmatrix}, \begin{pmatrix} 2-y-z \\ 3-x-2z \\ \text{something} \end{pmatrix}$$

Corollary 6.17 (Krull's Intersection Theorem 2.1.35). *Let A be a Noetherian ring, $I \subset A$ an ideal contained in the Jacobian radical and M a finitely generated A -module. Then*

$$\bigcap_{k \in \mathbb{N}} I^k M = \langle 0 \rangle$$

Proof. The A -module

$$N = \bigcap_k I^k M$$

is finitely generated, since M is Noetherian. By Nakayama's Lemma, it suffices to show that $IN = N$. \square

February 21

Let (A, \mathfrak{m}) be a local ring and M an A -module. A subset $\{m_1, \dots, m_n\} \subset M$ is a *minimal system of generators* if their classes form a basis of the vector space $M/\mathfrak{m}M$. A presentation $A^r \xrightarrow{\varphi} A^n \rightarrow M \rightarrow 0$ is *minimal* if $n = \dim_{A/\mathfrak{m}}(M/\mathfrak{m}M)$.

bf Exercise 2.1.17(p 111): The presentation above is minimal \iff

$$\varphi(A^r) \subset \mathfrak{m} \cdot A^n$$

This condition means that φ is the zero matrix modulo \mathfrak{m} , in which case its cokernel modulo \mathfrak{m} is n -dimensional. Otherwise, if φ has an entry that is not in \mathfrak{m} , then its cokernel modulo \mathfrak{m} has dimension $\leq n - 1$.

Example: in $A = \mathbb{Q}[x, y, z]_{\langle x, y, z \rangle}$

$$M = \text{coker} \begin{pmatrix} 0 & y \\ xy - 1 & xz \\ xy + 1 & xz \end{pmatrix}$$

Question: how to make a presentation minimal?

Answer: If $\varphi_{ij} \notin \mathfrak{m}$ we use elementary column operations to make entries of φ in row i zero, except φ_{ij} . These operations don't change M and its n generators. Now delete row i and column j to get a smaller presentation of M . Iterate...

In our example, we now have

$$M = \text{coker} \begin{pmatrix} 0 & y \\ xy - 1 & 0 \\ xy + 1 & \frac{2xz}{xy - 1} \end{pmatrix} = \text{coker} \begin{pmatrix} 0 & xy^2 - y \\ xy - 1 & 0 \\ xy + 1 & 2xz \end{pmatrix} \simeq \text{coker} \begin{pmatrix} xy^2 - y \\ 2xz \end{pmatrix}$$

In `Singular` we use the `PRUNE` command which doesn't change the structure:

```

> ring A=0,(x,y,z),ds;
> module M=[0,xy-1,xy+1],[y,xz,xz];
> print(M);
0,    y,
-1+xy,xz,
1+xy, xz
> print(prune(M));
-y+xy2,
-2xz

```

Definition 6.18 (2.1.38). Let A be a ring, and let $S \subset A$ be multiplicatively closed, and M an A -module.

1. The *localization* of M with respect to S is the $S^{-1}A$ -module

$$S \in M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\}$$

where $\frac{m}{s}$ is the class of $(m, x) \in M \times S$ where $(m, x) \sim (m', s') \iff \exists s'' \in S$ such that $s''(s'm - sm') = 0$.

2. Every A -module homomorphism $\varphi : M \rightarrow N$ gives an $S^{-1}A$ -module homomorphism

$$\varphi_S : M_S \rightarrow N_S, \quad \frac{m}{s} \mapsto \frac{\varphi(m)}{s}$$

Proposition 6.19 (2.1.37). *Just a few facts:*

- $\ker(\varphi_S) = \ker(\varphi)_S$
- $\text{im}(\varphi_S) \simeq \text{im}(\varphi)_S$
- $\text{coker}(\varphi_S) \simeq \text{coker}(\varphi)_S$

Proposition 6.20 (2.1.38). *The following are equivalent for an A -module M*

1. $M = \langle 0 \rangle$
2. $M_p = \langle 0 \rangle$ for all primes p
3. $M_{\mathfrak{m}} = \langle 0 \rangle$ for all maximal ideals \mathfrak{m} .

Proof. We need only show (3) \Rightarrow (1). Let $m \in M$ and assume $\text{Ann}(m) \subset \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Then $\frac{m}{1} \neq 0$ in $M_{\mathfrak{m}}$, which can't happen if (3) holds. Hence $1 \in \text{Ann}(m) \implies m = 0$ \square

Corollary 6.21 (2.1.39). *Let A be a ring and $\varphi : M \rightarrow N$ A -linear. Then φ is injective (respectively surjective) $\iff \varphi_{\mathfrak{m}}$ is injective (surjective) for all maximal ideals.*

$$A \left\{ \left(\begin{array}{cc} y & 0 \\ -x & z \\ 0 & -y \end{array} \right) \right\} \hookrightarrow \ker([x \ y \ z])$$

The *support* of a module M is

$$\text{supp}(M) = \{P \subset A \text{ prime ideals} \mid M_P \neq \langle 0 \rangle\}$$

Lemma 6.22 (2.1.41). *Let A be a ring and M is a finitely generated A -module. Then $\text{supp}(M) = \{P \subset A \text{ primes} \mid P \supset \text{Ann}(M)\}$.*

Proof. Assume $\text{Ann}(M) \not\subset P$ and pick $s \in \text{Ann}(M) \setminus P$. For any $m \in M$ we have $s \cdot m = 0$ in $M \implies \frac{m}{1} = \frac{sm}{s} = 0$ in M_P . Hence $M_P = \langle 0 \rangle$. Conversely, if $M_P = \langle 0 \rangle$, then $A_P = \text{Ann}(M_P) = \text{Ann}(M)_P$ (where the second equality is Exercise 2.1.24), hence $\text{Ann}(M) \not\subset P$. \square

Some Geometry: The above says that $\text{supp}(M)$ is the variety of $\text{Ann}(M)$ in the Zariski topology. For an example take

$$A = \mathbb{C}[a, b, c, d, e, f], \quad M_1 = \text{coker} \begin{bmatrix} a & d \\ b & e \\ c & f \end{bmatrix}, \quad M_2 = \text{coker} \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

where $\text{Spec}(A) = \mathbb{C}^6$. What are the annihilators and supports of these two modules? For M_2 , the annihilator is generated by 2×2 minors. The support consists of rank 1 matrices. Think about what happens when you quotient A by your favorite ideal.

7 Graded Rings and Modules (2.2)

A *graded ring* A is a ring together with a direct sum decomposition

$$A = \bigoplus_{\nu \geq 0} A_\nu$$

where the A_ν are abelian group satisfying

$$A_\nu A_\mu \subset A_{\nu+\mu} \text{ for } \nu, \mu \geq 0$$

A *graded K -algebra*, K a field, is a graded ring A where each A_ν is a K -vector space and $A_0 = K$. The A_ν are *homogeneous components* of A and the elements of A_ν are *homogeneous elements of degree ν* .

Example 7.1. $A = K[x_1, \dots, x_m]$, $w = (w_1, \dots, w_n) \in \mathbb{N}_+^n$.

$$A_\nu = K \cdot \{x^u : \underbrace{u_1 w_1 + \dots + u_n w_n}_{w\text{-degree}(x^u)} = \nu\}$$

Then $A = \bigoplus_{\nu \geq 0} A_\nu$ is a graded K -algebra. Now if $n = 4$, and $A = \mathbb{Q}[p, n, d, q]$, $w = (1, 5, 10, 25)$, what is $\dim_{\mathbb{Q}}(\bar{A}_{100})$? It's the number of ways of making change for a dollar. Now typically, if all $w_i = 1$ then we get the usual notion of homogeneity.

Let's end with a hard example (a 'blow-up'):

Example 7.2. If A is a (Noetherian) K -algebra and $I \subset A$ an ideal, then

$$\text{Gr}_I(A) = \bigoplus_{\nu \geq 0} I^\nu / I^{\nu+1} = A/I \oplus I^2/I \oplus \dots$$

is a graded ring in a natural way. How??? If (A, \mathfrak{m}) is a local ring then all homogeneous components of

$$\mathrm{Gr}_{\mathfrak{m}}(A) = \bigoplus_{\nu \geq 0} \mathfrak{m}^{\nu} / \mathfrak{m}^{\nu+1}$$

are finite dimensional vector spaces of A/\mathfrak{m} . FYI: this is much harder than you might think.

February 23

Let $A = \bigoplus_{\nu \geq 0} A_{\nu}$ be a graded ring $A_{\nu} = 0$ for $\nu > 0$. A *graded A -module* is a module with a direct sum decomposition

$$M = \bigoplus_{\mu \in \mathbb{Z}} M_{\mu}$$

into abelian groups such that $A_{\nu} \cdot M_{\mu} \subseteq M_{\nu+\mu}$ for all $\nu \in \mathbb{N}, \mu \in \mathbb{Z}$.

Example 7.3. Take $w = (w_1, \dots, w_m) \in \mathbb{Z}^m$. Then A^m is a graded module with degree $(e_i) = w_i$

$$(A^m)_{\nu} = \left\{ \sum_{i=1}^m a_i e_i \mid a_i \in A_{\nu-w_i} \text{ for all } i \right\}$$

Definition 7.4 (2.2.6). (Important) Let M be a graded module, $d \in \mathbb{Z}$. The *d -shift* of M is the graded module

$$M(d) = \bigoplus_{\nu \in \mathbb{Z}} M(d)_{\nu}$$

where $M(d)_{\nu} = M_{d+\nu}$.

Example 7.5. $S = \mathbb{Q}[x, y]$ with the usual $(1, 1)$ -grading. $M = S(-3) \oplus S(2)$, ungraded S^2 . What are

$$\begin{aligned} \dim_{\mathbb{Q}}(M_{-1}) &= 2 & \{(0, x), (0, y)\} \\ \dim_{\mathbb{Q}}(M_1) &= 4 & \{(0, x^3), (0, x^2y), (0, xy^2), (0, y^3)\} \\ \dim_{\mathbb{Q}}(M_4) &= 2 + 7 = 9 & \{(x, 0), (y, 0), (0, x^i y^j) \mid i + j = 6\} \end{aligned}$$

Lemma 7.6 (2.2.7). Let $M = \bigoplus_{\nu \in \mathbb{Z}} M_{\nu}$ be a graded A -module and $N \subset M$ a submodule. The following are equivalent:

1. N is graded with the induced grading, i.e. $N = \bigoplus_{\nu \in \mathbb{Z}} (M_{\nu} \cap N)$
2. N is generated by homogeneous elements
3. If $m = \sum m_{\nu}$, $m_{\nu} \in M_{\nu}$, then $(m \in N \iff m_{\nu} \in N \text{ for all } \nu)$

A submodule $N \subset M$ is *homogeneous* (or *graded*) if it satisfies (1),(2),(3). The same goes for ideals $I \subset A$.

If I is a homogeneous ideal in a graded ring $A = \bigoplus_{\nu \geq 0} A_{\nu}$ then the quotient is a graded ring $A/I \simeq \bigoplus_{\nu \geq 0} A_{\nu} / (I \cap A_{\nu})$.

Example 7.7. Take $A = \mathbb{Q}[p, n, d, q]$ graded by $w = (1, 5, 10, 25)$. The following ideals are homogeneous:

$$\begin{aligned} I &= \langle q + nd^2 + dnp^{10} + p^{25} \rangle \\ J &= \langle p^{25} - q, p^{10} - d, p^5 - n \rangle, A/J \simeq \mathbb{Q}[t] \end{aligned}$$

Note: suppose we have a polynomial ring that's graded. Then all reduced Gröbner bases of a homogeneous ideal consist of homogeneous polynomials.

For a reduced Gröbner basis, any non-leading term in a homogeneous polynomial was not in the ideal.

Definition 7.8 (2.2.10). Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a graded ring and $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ and $N = \bigoplus_{\nu \in \mathbb{Z}} N_\nu$ graded modules. (Note we can take ν, μ in any abelian group other than the integers). A homomorphism $\varphi : M \rightarrow N$ is *homogeneous (or graded) of degree d* if $\varphi(M_\nu) \subset N_{\nu+d}$ for all ν . If $d = 0$ then φ is *homogeneous*.

Example 7.9 (2.2.11). If M is a graded A -module and $f \in A_d$, then multiplication by f defines a graded homomorphism $M \rightarrow M$ of degree d . It also defines graded (or homogeneous) homomorphisms $M \rightarrow M(d)$ or $M(-d) \rightarrow M$ (this notation is inconsistent with matrix multiplication so typically in commutative algebra and **Singular**, we use the notation $M \xleftarrow{f} M(-d)$).

$S = \mathbb{Q}[x, y]$ with usual $(1, 1)$ -grading. What are the graded (of degree $d = 0$) homomorphisms?

$$S(-3) \oplus S(-1) \rightarrow S(-4) \oplus S(-1) \oplus S$$

(A map like this is given by a 3×2 matrix) First we can say it's a subset of $\text{Hom}(S^2, S^3) \simeq S^6$. It's not a submodule because if multiply by say x , we'll change it. It's a finite dimensional \mathbb{Q} -vector space of dimension 10 with basis. You should use the names of the bases. Use the

`\bordermatrix`

command in latex.

$$\begin{bmatrix} 0 & 0 \\ x, xy, y^2 & 1 \\ x^3, \dots, y^3 & x \text{ or } y \end{bmatrix}$$

Gives $S(-3)$ and $S(7)$

Lemma 7.10 (2.2.12). Let $\varphi : M \rightarrow N$ be a homogeneous A -module homomorphism. Then $\ker(\varphi), \text{im}(\varphi)$ and $\text{coker}(\varphi)$ are A -modules with the induced grading.

Now to do a little of the homework. For the last problem, 2.2.7, we have

$$\langle y^5 - z^2, x^3 - z, x^6 - y^5 \rangle, \langle y^5 - z^2, x^3 - z, x^7 - y^5 \rangle \subset K[x, y, z]$$

Test whether these are homogeneous ideals in $K[x, y, z]$ with respect to suitable *weights*. And the other one, 2.2.4, I_1, I_2 homogeneous ideals in a graded ring. Show that $I_1 + I_2, I_1 \cap I_2, I_1 \cdot I_2, I_1 : I_2$ and \sqrt{I} are homogeneous. Well product is clearly still homogeneous. For the first one, it can be solved with a certain algorithm.

March 9

8 Hilbert function and Hilbert Polynomial & Computation of the Hilbert-Poincaré series

A Noetherian graded K -algebra, M a finitely generated graded A -module. The *Hilbert function*

$$H_M : \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto \dim_K(M_n)$$

The *Hilbert-Poincaré series* of M is the generating function

$$HP_M(t) = \sum_{\nu \in \mathbb{Z}} H_M(\nu) \cdot t^\nu \in \mathbb{Z}[[t]][t^{-1}]$$

Lemma 8.1 (5.1.2). 1. If $N \subset M$ is a graded submodule then

$$H_M(n) = H_N(n) + H_{M/N}(n) \text{ for all } n$$

and hence $HP_M(t) = HP_N(t) + HP_{M/N}(t)$

2. For any integer d , $H_{M(d)}(n) = H_M(n + d)$ for all n , and hence $HP_{M(d)}(t) = t^{-d} \cdot HP_M(t)$

3. Let $f \in A_d$ and consider $\varphi : M(-d) \xrightarrow{f} M$. Then $\ker(\varphi)$ and $\text{coker}(\varphi)$ are graded $A/\langle f \rangle$ -modules and

$$H_M(n) - H_M(n - d) = H_{\text{coker}(\varphi)}(n) - H_{\ker(\varphi)}(n - d)$$

Hence $HP_M(t) - t^d HP_M(t) = HP_{\text{coker}(\varphi)}(t) - t^d HP_{\ker(\varphi)}(t)$

Theorem 8.2 (5.1.3). Let A be a graded K -algebra, which is generated by $x_1, x_2, \dots, x_r \in A_1$. Then for any finitely generated (positively) graded A -module $M = \bigoplus_{n \geq 0} M_n$, we have

$$HP_M(t) = \frac{Q(t)}{(1-t)^r} \text{ for some } Q \in \mathbb{Z}[t]$$

Proof. Induction on r . If $r = 0$, M is a finite-dimensional K -vector space.

$$M = M_0 \oplus M_1 \oplus \dots \oplus M_s \mid HP_M(t) = Q(t) = \sum_{\nu=0}^s \dim_K(M_\nu) t^\nu$$

For $r > 0$, consider $\varphi : M(-1) \xrightarrow{x_1} M$. This implies

$$(1-t)HP_M(t) = HP_{\text{coker}(\varphi)}(t) - t \cdot HP_{\ker(\varphi)}(t)$$

Both $\ker(\varphi)$ and $\text{coker}(\varphi)$ are graded modules over $A/\langle x_1 \rangle = A_0[\bar{x}_2, \dots, \bar{x}_r]$ Induction gives

$$\begin{aligned} HP_{\text{coker}(\varphi)}(t) &= Q_1(t)/(1-t)^{r-1} \\ HP_{\ker(\varphi)}(t) &= Q_2(t)/(1-t)^{r-1} \end{aligned}$$

□

Write

$$HP_M(t) = \frac{Q(t)}{(1-t)^r} = \frac{G(t)}{(1-t)^s}$$

where $Q(t)$, resp. $G(t)$, is called the *first Hilbert series*, resp. *second Hilbert series*, with $s \leq r$ and

$$G(t) = \sum_{\nu=0}^d g_{\nu} t^{\nu} \in \mathbb{Z}[t]$$

has no zero at $t = 1$.

So the *Hilbert polynomial* of M is

$$P_M(n) = \sum_{\nu=0}^d g_{\nu} \cdot \binom{s-1+n-\nu}{s-1} \in \mathbb{Q}[n]$$

Corollary 8.3 (5.1.5). $P_M(n) = H_M(n)$ for all $n \geq d$, where d is called the *regularity*

Proof.

$$\begin{aligned} HP_M(t) &= \left(\sum_{\nu=0}^d g_{\nu} t^{\nu} \right) \left(\sum_{\mu=0}^{\infty} \binom{s-1+\mu}{s-1} t^{\mu} \right) \\ &= \text{Stuff of degree } \leq d + \sum_{n=d}^{\infty} \left(\sum_{\lambda=0}^d g_{\lambda} \binom{s-1+n-\lambda}{s-1} \right) t^n \end{aligned}$$

□

Example 8.4 (twisted cubic curve). $A = K[x_1, x_2, x_3, x_4]$,

$$\begin{aligned} I &= \langle \underline{x_2^2} - x_1 x_3, \underline{x_2 x_3} - x_1 x_4, \underline{x_3^2} - x_2 x_4 \rangle \\ &= 2 \times 2\text{-minors of } \begin{bmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \end{bmatrix} \end{aligned}$$

and $M = A/I$. A K -basis for M is given by the *standard monomials*

$$\{1, x_2, x_3\} \cdot x_1^* x_4^*$$

The Hilbert function H_M is

$$\begin{array}{cccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ H_M(n) & 1 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}$$

The Hilbert-Poincaré series

$$HP_M(t) = \frac{1 - 3t^2 + 2t^3}{(1-t)^4}$$

which gives the resolution

$$0 \rightarrow A(-3)^2 \rightarrow A(-2)^3 \rightarrow A \rightarrow M \rightarrow 0$$

The second Hilbert series is $\frac{1+2t}{(1-t)^2}$. We have $s = 2 = \text{“Krull dimension of } A/I\text{”}$, $d = 1 = \text{“regularity”}$
 Now let's calculate the Hilbert polynomial.

$$P_M(n) = 1 \binom{1+n}{1\dots} + 2 \binom{1+n-1}{1} = (1+n) + 2n = 3n+1$$

Algorithm 8.5 (5.2.8). Input: A homogeneous ideal $I \subset K[x_1, \dots, x_r]$

Output: The Hilbert-Poincaré of $K[\bar{x}]/I$.

Method: Compute any Gröbner basis and apply Algorithm 5.2.4 to the monomial ideal $M = L(I)$ and count the standard monomials. (note that $K[\bar{x}]/I$ and $K[\bar{x}]/L(I)$ are the same as vector spaces but very, very different as rings)

Lemma 8.6 (5.2.2). $I \subset K[\bar{x}]$ a homogeneous ideal, $f \in K[\bar{x}]_d$.

$$HP_{K[\bar{x}]/I}(t) = HP_{K[\bar{x}]/\langle I, f \rangle}(t) + t^d \cdot HP_{K[\bar{x}]/(I:f)}(t)$$

Note that if you can find an f that splits, that's very good news, esp. in chapter 4.

Proof. Use the short exact sequence

$$0 \rightarrow \frac{K[\bar{x}]}{(I:f)}(-d) \xrightarrow{f} \frac{K[\bar{x}]}{I} \rightarrow \frac{K[\bar{x}]}{\langle I, f \rangle} \rightarrow 0$$

□

Algorithm 8.7 (5.2.4). Input: $I = \langle m_1, \dots, m_k \rangle$, m_i monomials in x_1, \dots, x_r .

Output: A polynomial $Q(t)$ such that

$$HP_{K[\bar{x}]/I} = \frac{Q(t)}{(1-t)^r}$$

- Minimalize I
- If m_1, \dots, m_k are distinct variables, return $Q(t) = (1-t)^k$.
- Otherwise, *pick* $x_i \notin I$, which appears in a minimal generator
- Apply recursively to $\langle I, x_i \rangle$ and $(I : x_i)$ and add result.

Now why would such a thing terminate? By some Noetherian argument...

March 14

David Eisenbud: Free resolutions in geometry

Have $S = k[x_0, \dots, x_r]$, with k a field, M a finitely generated graded module. Have the free resolution:

$$0 \leftarrow M \leftarrow F_0 \leftarrow \dots \leftarrow F_n \leftarrow 0$$

with F_i free, and the maps are homogeneous of degree 0. M is generated by elements of degrees d_1, \dots, d_s . Choose $F_0 = \bigoplus_i S(-d_i)$. F_i is a free graded module with $F_i = \bigoplus S(-j)^{\beta_{i,j}}$.

The Kozul complex is the mother of all complexes.

$$\begin{array}{l} \mathbb{K}(x) \quad \mathbb{F} \quad S(-1) \xleftarrow{x} S(-2) \leftarrow 0 \\ \mathbb{K}(x, y) \quad \mathbb{G} \quad S \xleftarrow{x} S(-1) \leftarrow 0 \end{array}$$

Whenever you have two complexes and a map in between them, you can have the mapping cone. (diagram)

Proposition 8.8. Given two resolutions \mathbb{F}, \mathbb{G} of modules A and B with mapping cone $\phi : \mathbb{F} \rightarrow \mathbb{G}$, then \mathbb{M} is a resolution of $B/A \iff H_0 \mathbb{F} \rightarrow H_0 \mathbb{G}$ is a monomorphism.

$$\text{Now } \mathbb{K}(x_0, \dots, x_r) = \mathbb{M}(\mathbb{K}(x_0, \dots, x_{r-1}) \xrightarrow{x_r} \mathbb{K}(x_0, \dots, x_{r-1})).$$

Corollary 8.9. $\mathbb{K}(x_0, \dots, x_r)$ is a free resolution of $S/(x_0, \dots, x_r) = k$.

So the Kozul complex in three variables looks like:

$$S \xleftarrow{(x,y,z)} S^3(-1) \begin{pmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{pmatrix} \xleftarrow{\quad} S^3(-2) \begin{pmatrix} x \\ y \\ z \end{pmatrix} \xleftarrow{\quad} S$$

Now we'll look at the Hilbert function, $H_M(d) = \dim_k M_d$. Then

$$H_M(d) = \sum (-1)^i H_{F_i}(d)$$

But $H_{F_i}(d) = \sum \beta_{ij} H_{S(-j)}(d)$ and

$$H_{S(-j)}(d) = H_S(d-j) = \binom{r+d-j}{r} = \frac{\overbrace{(r+(d-j))(r+d-j-1)\dots}^r}{r!}$$

So $H_M(d)$ is a polynomial in d when $d \geq j - r$ for all j such that $\beta_{ij} \neq 0$.

One way to think of resolutions is as isomorphisms in some other category. Given the resolution $k \leftarrow \mathbb{K}(x_0, \dots, x_r)$, we have

$$M = M \otimes_k k \leftarrow M \otimes_k \mathbb{K}(x_0, \dots, x_r).$$

So every module has a free resolution which is just the Kozul complex.

What does the size of a resolution mean?

1. If \mathbb{F}, \mathbb{F}' are minimal free resolutions of M (choose minimal number of generators at each step), then $\mathbb{F} \cong \mathbb{F}'$. (easy, but slightly messy)
2. length of the minimal free resolution = projective degree of $M = r + 1 - \text{depth of } M$.

3. (Castelnuovo-Mumford) regularity of $M = \max\{j - i \mid \beta_{ij} \neq 0\}$ = index of last row in betti diagram.

March 16

9 Computing resolutions

[2.5] R any ring, M and R -module. A *syzygy* (or relation) between $f_1, \dots, f_k \in I$ is any element in the kernel of $\varphi : R^k \rightarrow M$ with $e_i \mapsto f_i$, and $\ker(\varphi) =: \text{syz}(f_1, \dots, f_k)$, $I := \langle f_1, \dots, f_k \rangle_M$.

Remark 9.1 (2.5.2). If R is local (or graded) and $\{f_1, \dots, f_k\}$ and $\{g_1, \dots, g_k\}$ are minimal generators for I then

$$\text{syz}(f_1, \dots, f_k) \simeq \text{syz}(g_1, \dots, g_k) =: \text{syz}(I)$$

We define iteratively the k -th syzygy module of I as $\text{syz}_0(I) = I$ and $\text{syz}_k(I) := \text{syz}(\text{syz}_{k-1}(I))$ for $k \geq 0$.

The k -th *Betti number* $b_k(I)$ is the minimal number of generators of $\text{syz}_k(I)$. In the graded case, the *graded Betti numbers* $b_{j,k}(I)$ is the minimal number of generators of $\text{syz}_k(I)$ in degree $j + k$.

So how do we compute them? Method 1 for computing syzygies for submodules of R^r where $R = k[x_1, \dots, x_n]$, $I = \langle f_1, \dots, f_k \rangle \subset R^r$. Use Gröbner bases in

$$R^{r+k} = \underbrace{\bigoplus_{i=1}^r Re_i}_{(*)} \oplus \bigoplus_{j=r+1}^{r+k} Re_j$$

We can now think of this as computation in $r + k + n$ variables even though you can't multiply e_i with e_j .

The *Monomial order* $(c, >)$ is defined by

$$x^a e_i < x^b e_j \text{ if } i > j \text{ or } (i = j \text{ and } x^a < x^b)$$

This is called "POT" which is ordering "Position Over Term". You can also have "TOP" (Term Over Position) which we won't do here.

Algorithm 9.2 (2.5.4). **Input:** $f_1, \dots, f_k \in K[\bar{x}]^r$, $>$ monomial ordering on $K[\bar{x}]$.

Output: A subset of $K[\bar{x}]^r = (*)$ which generates $\text{syz}(f_1, \dots, f_k)$

- Compute a Gröbner basis G of $\{f_1 + e_{r+1}, f_2 + e_{r+2}, \dots, f_k + e_{r+k}\}$
- Output $G \cap \bigoplus_{j=r+1}^{r+k} e_j$

Example 9.3. $r = 1, k = 3, n = 4$ with $(x_2^2 - x_1x_3, 1, 0, 0) = A$, $(x_2x_3 - x_1x_4, 0, 1, 0) = B$, $(x_3^2 - x_2x_4, 0, 0, 1) = C$. Now $x_3A - x_2B = (x_1x_2x_4 - x_1x_3^2, x_3, -x_2, 0)$. Adding x_1C to get $(0, x_3, -x_2, x_1)$ and also $(0, x_4, -x_3, x_2)$ which are both in $G \cap \bigoplus_{j=2}^4 Re_j$. Look up the *Hilbert-Burch Theorem*.

By iterating Alg 2.5.4, we can compute a minimal free resolution of I . Since we're graded or local, you can't get stuck along the way by introducing a non-zero constant. Correctness follows from the elimination property of $(c, >)$.

A more systematic (Gröbner friendly) method for constructing resolutions is *Schreyer's Algorithm* ("Lifting Syzygies" -Eisenbud Chapter 13) and prove Buchberger's Criterion.

Let $I = \langle f_1, \dots, f_k \rangle \subset R^r = F_0$ with a monomial order $>_0$. The *Schreyer ordering* $>_1$ on $R^k = F_1$ is defined as follows

$$x^\alpha \varepsilon_1 >_1 x^\beta \varepsilon_j \iff \text{LM}(x^\alpha f_i) >_0 \text{LM}(x^\beta f_j) \text{ or } (\text{LM}(x^\alpha f_i) = \text{LM}(x^\beta f_j) \text{ and } i < j)$$

If f_i and f_j ($i < j$) have their leading terms in the same component, say $\text{LM}(f_i) = x^{\alpha_i} e_\nu$ and $\text{LM}(f_j) = x^{\alpha_j} e_\nu$ and $\gamma = \text{lcm}(\alpha_i, \alpha_j)$ (may assume $\alpha_j > \alpha_i$ lexicographically (**))

$$m_{ji} = x^{\gamma - \alpha_i}, c_i = \text{LC}(f_i), c_j = \text{LC}(f_j)$$

$\text{spoly}(f_i, f_j) = m_{ji} f_i - \frac{c_i}{c_j} m_{ij} f_j \in F_0$. Assume we have standard representation

$$\text{spoly}(f_i, f_j) = \sum_{\nu=1}^k a_{n\nu}^{(ij)} f_\nu \in F_0$$

Then we define

$$s_{ij} := m_{ji} \varepsilon_i - \frac{c_i}{c_j} m_{ij} \varepsilon_j - \sum_{\nu=1}^k a_{n\nu}^{(ij)} \varepsilon_j \in \text{syz}(I) \subset F_1$$

Now the Schreyer order is defined to make the following lemma true.

Lemma 9.4 (2.5.8). $LM_{<_1}(s_{ij}) = m_{ji} \varepsilon_i$

Theorem 9.5 (2.5.9). Let $G = \{f_1, \dots, f_k\}$ be generators of $I \subset R^r$. Let

$$M = \{(i, j) | 1 \leq i < j \leq k, \text{LM}(f_i) \text{ and } \text{LM}(f_j) \text{ are in some slot } \nu\}$$

and $\mathcal{J} \subseteq M$ such that

- $NF(\text{spoly}(f_i, f_j), G) = 0$ for all $(i, j) \in \mathcal{J}$
- $\langle \{m_{ji} \varepsilon_i | (i, j) \in \mathcal{J}\} \rangle = \langle \{m_{ji} \varepsilon_i | (i, j) \in M\} \rangle \in R^k$.

Then

1. G is a standard basis of I with respect to $<_0$ (Buchberger's Criterion)
2. $S = \{s_{ij} | (i, j) \in \mathcal{J}\}$ is a standard basis for $\text{syz}(I)$ with respect to the Schreyer ordering $<_1$. In particular, they generate

This implies the Chain Criterion (2.5.10). Buchberger's first and second criterion implies how to chose \mathcal{J} avoiding unnecessary S-pairs. The second criterion in the theorem above is so clever that you only have to take adjacent S-pairs. Now to use (**).

Lemma 9.6 (2.5.14). Let $G = \{g_1, \dots, g_r\}$ be a standard basis of $I \subset R^r$ ordered such that (**) holds. Suppose $LM_{>_0}(g_1), \dots, LM_{>_0}(g_s)$ do not depend on x_1, \dots, x_k . Then the $LM_{>_1}(s_{ij})$ do not depend on x_1, \dots, x_{k+1} .

Note that the Schreyer order is determined by the old term order and the order in which you write down g_1, \dots, g_s .

Proof. $\alpha_i = (0, \dots, 0, *, \dots, ?)$, $\alpha_j = (\underbrace{0, \dots, 0}_k, *, \dots, ?) \in \mathbb{N}^n$ and use (**) on the *-component. Therefore $\text{LM}(s_{ij}) = m_{ji}\varepsilon_i = x^{\text{lcm}(\alpha_i, \alpha_j) - \alpha_i} \varepsilon_i$ does not depend on x_{k+1} . \square

Corollary 9.7 (Hilbert's Syzygy Theorem). *Every finitely generated $K[x_1, \dots, x_n]$ -module M has a free resolution of length $m \leq n$:*

$$0 \rightarrow F_m \rightarrow F_{m-1} \rightarrow \dots \rightarrow F_0 \rightarrow M \rightarrow 0$$

Example 9.8. $n = 2$:

$$0 \rightarrow F_2 \rightarrow F_1 \xrightarrow{I} F_0 \rightarrow M \rightarrow 0$$

For any submodule $I \subset K[x, y]^r$, the syzygy module is free.

Question: Why did Hilbert prove the H.S.T.?

Answer: *Invariant Theory* - this was the hardest topic in the 19th century.

March 21

10 Operations on Modules and their Computation (2.8)

$R = K[x_1, \dots, x_n]_{>}$

10.1 Module Membership (2.8.1)

Problem: Given $f_1, \dots, f_k \in R^r$, decide whether $f \in \langle f_1, \dots, f_k \rangle$ and if so, exhibit a representation.

Solution: Compute a standard basis of $\langle f_1, \dots, f_k \rangle$, and then take the normal form of f . $\text{NF} = 0 \iff$ it is in the module and keeping track gives the representation.

10.2 Elimination of module components (2.8.2)

In Singular, use the POT order $(c, >)$.

10.3 Intersection of Submodules (2.8.3)

Problem: Given $I_1 = \langle f_1, \dots, f_k \rangle$ and $I_2 = \langle h_1, \dots, h_s \rangle$ in R^r , compute generators for $I_1 \cap I_2$.

Solution: Compute generators for the kernel of the $2r \times (r + k + s)$ -matrix

$$\begin{bmatrix} I & f_1 & \dots & f_k & 0 & \dots & 0 \\ I & 0 & \dots & 0 & g_1 & \dots & g_s \end{bmatrix}$$

and project as in 2.8.2 onto the first r coordinates.

Example 10.1. $k = 1 = s$, $r = 1$, $n = 2$, $I_1 = \langle x^2 \rangle$, $I_2 = \langle xy \rangle$, $I_1 \cap I_2 = \langle x^2y \rangle$. Idea: Use syzygies.

$$\ker \begin{bmatrix} 1 & x^2 & 0 \\ 1 & 0 & xy \end{bmatrix} = \left\langle \begin{pmatrix} x^2y \\ -y \\ -x \end{pmatrix} \right\rangle$$

10.4 Quotients of Submodules (2.8.4)

Problem: Give submodules $I_1 = \langle f_1, \dots, f_k \rangle$ and $I_2 = \langle h_1, \dots, h_s \rangle$ in R^r , compute generators of

$$I_1 : I_2 = \{g \in R \mid gI_2 \subset I_1\} = \text{Ann} \left(\frac{(I_1 + I_2)}{I_1} \right)$$

Solution: Compute the kernel of the $sr \times (1 + sk)$ -matrix

$$\begin{bmatrix} h_1 & f_1 & \cdots & f_k & 0 & \cdots & 0 & & 0 \\ h_2 & 0 & \cdots & 0 & f_1 & \cdots & f_k & & \vdots \\ \vdots & & \vdots & & 0 & \cdots & 0 & \ddots & 0 \\ h_s & 0 & \cdots & 0 & 0 & \cdots & 0 & & f_1 \cdots f_k \end{bmatrix}$$

and project onto the first coordinate.

Example 10.2. $r = k = s = 1$, $n = 2$, $I_1 = \langle x^2 \rangle$, $I_2 = \langle xy \rangle$.

$$\ker[xy \ x^2] = \left\langle \begin{pmatrix} x \\ -y \end{pmatrix} \right\rangle$$

How about over $A = R/I$? Well the variant for modules given by generators and relations.

Problem: Let $A = R/I$, $\pi : R \rightarrow A$ and $\varphi : M_1 \rightarrow M_2$ defined by three matrices B, B_1, B_2 as follows:

$$A^r \xrightarrow{B_1} A^p \rightarrow M_1 \rightarrow 0$$

$$A^s \xrightarrow{B_2} A^q \rightarrow M_2 \rightarrow 0$$

with $B : A^p \rightarrow A^q$. Compute

$$\begin{aligned} \varphi(M_1) :_A M_2 &= \text{Ann}_A(M_2/\varphi(M_1)) \\ &= \langle \text{columns of } B \text{ and of } B_2 \rangle :_A \langle e_1, \dots, e_q \rangle \\ &= \pi(\langle \text{---} \rangle + I \cdots R^q) :_R \langle e_1, \dots, e_q \rangle \end{aligned}$$

10.5 Annihilator and Support (2.8.6)

Problem: Given an ideal $I = \langle f_1, \dots, f_k \rangle \subset R$ and a module M over $A = R/I$. Compute generators for the ideal $\text{Ann}_A(M)$.

Aside: Now communicating such things as vector bundles, line bundles and sheafs with the computer we have to realize these concepts as modules.

Case 1: $M \subset A^r$ is given by generators $m_1, \dots, m_s \in R^r$.

Case 2: M is given as cokernel

$$A^p \xrightarrow{B} A^q \rightarrow M \rightarrow 0$$

Solution 1: Compute $\langle 0 \rangle :_A M$ as in 2.8.4, but with $A = R/I$ as base ring, i.e. compute $(I \cdot R^r) :_R \langle m_1, \dots, m_s \rangle$ and project mod I . (we just learned how to do this if A were R , and this is even easier).

Example 10.3. $I = \langle u(x, y), v(x, y) \rangle \subset \mathbb{Q}[x, y] = R$.

$$M = \text{im} \begin{pmatrix} m_{11}(, xy) & m_{12}(, xy) & m_{13}(, xy) \\ m_{21}(, xy) & m_{22}(, xy) & m_{23}(, xy) \end{pmatrix}$$

$$I \cdot R^2 = \text{im} \begin{pmatrix} u & v & 0 & 0 \\ 0 & 0 & u & v \end{pmatrix}$$

Compute the kernel of

$$\begin{bmatrix} m_{11} & u & v & 0 & 0 & 0 & 0 \\ m_{21} & 0 & 0 & u & v & 0 & 0 \\ m_{12} & & & 0 & & u & v & 0 & 0 \\ m_{22} & & & 0 & & 0 & 0 & u & v \\ m_{13} & & & 0 & & & & u & v & 0 & 0 \\ m_{23} & & & 0 & & & & 0 & 0 & u & v \end{bmatrix}$$

Solution 2: $M \simeq A^q / \text{im}(B) \implies \text{Ann}_A(M) = \text{im}(B) :_A A^q$. Use 2.8.4 to compute

$$(\langle \text{columns of } B \rangle + I \cdot R^q) :_R \langle e_1, \dots, e_q \rangle$$

and then project onto A .

Example 10.4. $M = \text{coker} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$. Compute the kernel of

$$\begin{bmatrix} e_1 & b_{11} & b_{12} & b_{13} & u & v & 0 & 0 \\ & b_{21} & b_{22} & b_{23} & 0 & 0 & u & v \\ e_2 & & 0 & & 0 & & b_{11} & b_{12} & b_{13} & u & v & 0 & 0 \\ & & & & & & b_{21} & b_{22} & b_{23} & 0 & 0 & u & v \\ & & & & & & & & & b_{11} & b_{12} & b_{13} & u & v & 0 & 0 \\ & & & & & & & & & b_{21} & b_{22} & b_{23} & 0 & 0 & u & v \end{bmatrix}$$

then project onto 1st coordinate, then to $A = R/I$.

Example 10.5. $A = R = \mathbb{Q}[a, b, c, d, e, f]$, $I = \langle 0 \rangle$, $B = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$. The kernel of

$$\begin{bmatrix} 1 & a & b & c & 0 & 0 & 0 \\ 0 & d & e & f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & b & c \\ 1 & 0 & 0 & 0 & d & e & f \end{bmatrix}$$

contains $\underbrace{[ae - bd, e, -d, 0, b, -a, 0]}_{\text{etc.}}$. This implies $\text{Ann}_A(\text{coker}(B)) = \text{ideal of } 2 \times 2\text{-minors of } B$.

There only remains 2.8.7 Kernel of a module homomorphism and 2.8.8 Solving Linear equations.

At the recent winter school in Arizona, Mike Stillman, who is the author of *M2* (McCauley 2), a program like **Singular**, gave a course on “Computing Sheaf Cohomology”. You can probably find the notes online.

Q: What comes after Greuel-Pfister?

Well there are two books: Eisenbud’s “Geometry of Syzygies” and Mike Stillman’s “Combinatorial Commutative Algebra” But these books don’t talk about how to calculate if a module is free. T. Lambe here is writing a great book on this now.

Now consider the furry coconut: $A = \mathbb{R}[x, y, z]/\langle x^2 + y^2 + z^2 - 1 \rangle$. The $\ker(x \ y \ z)$ is projective (looks like free) but is not free.

March 23

11 Tensor Products (2.7)

Definition 11.1. M, N modules over A . Their *tensor product* $M \otimes_A N$ is the free module generated by the symbols $\{m \otimes n | m \in M, n \in N\}$ modulo the relations

1. $(am) \otimes n = m \otimes (an) = a \cdot (m \otimes n)$
2. $(m + m') \otimes n = m \otimes n + m' \otimes n$
3. $m \otimes (n + n') = m \otimes n + m \otimes n'$

Example 11.2. $A = \mathbb{Z}$, $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^3 = \mathbb{Z}^6$, $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^2$, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}^3 = (\mathbb{Z}/2\mathbb{Z})^3$, and $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{R} = 0$.
 $1 \otimes r = 1 \otimes (2 \cdot \frac{r}{2}) = 2 \otimes (\frac{r}{2}) = 0 \otimes \frac{r}{2} = 0$

Definition 11.3. Tensor product turns bilinear maps into linear maps. A map $\sigma : M \times N \rightarrow P$ is *bilinear* if

1. $\sigma(am, n) = \sigma(m, an) = a \cdot \sigma(m, n)$
2. $\sigma(m + m', n) = \sigma(m, n) + \sigma(m', n)$
3. $\sigma(m, n + n') = \sigma(m, n) + \sigma(m, n')$

Write $B(M, N, P)$ for the modules of such bilinear maps.

Proposition 11.4. *There are canonical isomorphisms of A -modules:*

1. $B(M, N, P) \simeq \text{Hom}_A(M \otimes_A N, P)$
2. $B(M, N, P) \simeq \text{Hom}_A(M, \text{Hom}_A(N, P))$

Proof. 1. Define $\phi : \text{Hom}(M \otimes_A N, P) \rightarrow B(M, N, P)$ by $\phi(\varphi)(m, n) = \varphi(m \otimes n)$. Well-defined by definition of tensor product. If $\phi(\varphi) = 0$, then $\varphi(m \otimes n) = 0$ for all m, n . Since $M \otimes_A N$ is generated by such elements, we have $\varphi = 0 \implies \phi$ is injective. To see that ϕ is surjective let $\sigma \in B(M, N, P)$ and define a linear map φ from $M \otimes_A N$ to P by $\varphi(m \otimes n) = \sigma(m, n)$. This is well-defined and A -linear by definition of bilinear. Hence ϕ is an isomorphism.

2. Proof here is similar

□

Question: Aren't all elements of $M \otimes_A N$ of the form $m \otimes n$?

Answer: No, consider $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{Z}^3$ with $\{e_1, e_2\}$ a basis for \mathbb{Z}^2 and $\{f_1, f_2, f_3\}$ a basis for \mathbb{Z}^3 . The elements are $\sum_{i=1}^2 \sum_{j=1}^3 a_{ij}(e_i \otimes f_j)$ and can be written as 2×3 -matrices (a_{ij}) . The *decomposable* elements are

$$m \otimes n = \left(\sum_{i=1}^2 b_i e_i \right) \otimes \left(\sum_{j=1}^3 c_j f_j \right) = \sum_i \sum_j b_i c_j (e_i \otimes f_j)$$

so they are rank 1 matrices.

Question: In $\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^2$ (if mathematician or physicist, call these 2x2x2x2-tensors, computer scientist, call them four qubits, and statistician call these 2^4 -table), what are the elements of tensor rank 2?

Answer: Math 127 (Math Bio) - ask Anne or Jeff the answer.

Easy Results: (Prop 2.7.3, Ex 2.7.4)

1. $A^r \otimes_A A^s \simeq A^{rs}$, with basis $\{e_i \otimes f_j\}$
2. $M \otimes_A N \simeq M \otimes_A N$
3. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$
4. $A \otimes_A M \simeq M$
5. $(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$
6. $S^{-1}(M \times_A N) \simeq S^{-1}M \otimes_A S^{-1}N$
7. If $\varphi : M \rightarrow M$ and $\psi : N \rightarrow N$ are A -linear maps, then we get an A -linear map

$$(\varphi \otimes \psi) : M \otimes_A N \rightarrow M' \otimes_A N' \text{ where } m \otimes n \mapsto \varphi(m) \otimes \psi(n)$$

8. For two linear maps between free modules $\varphi : A^r \rightarrow A^s$ and $\psi : A^p \rightarrow A^q$, the matrix of $(\varphi \otimes \psi) : A^{rp} \rightarrow A^{sq}$ has entries $\varphi_{ij}\psi_{kl}$ in row (i, k) and column (j, l) .

These can be used to compute tensor products like

$$\text{im}(\varphi) \otimes_A \text{im}(\psi) = \text{im}(\varphi \otimes_A \psi)$$

Theorem 11.5 (2.7.6). “*Tensor product is right exact*” If

$$M \xrightarrow{i} N \xrightarrow{\pi} P \rightarrow 0$$

is an exact sequence of A -modules and L any A -module, then

$$M \otimes_A L \xrightarrow{i \otimes \text{id}_L} N \otimes_A L \xrightarrow{\pi \otimes \text{id}_L} P \otimes L \rightarrow 0$$

is exact.

Proof. By Prop 2.4.3, we need only show

$$0 \rightarrow \text{Hom}_A(P \otimes L, S) \rightarrow \text{Hom}(N \otimes L, S) \rightarrow \text{Hom}(M \otimes L, S)$$

is exact for all S . But by Prop 2.7.2 (2), we need only show

$$0 \rightarrow \text{Hom}_A(P, \text{Hom}_A(L, S)) \rightarrow \text{Hom}_A(N, \text{Hom}_A(L, S)) \rightarrow \text{Hom}_A(M, \text{Hom}_A(L, S)) \quad \forall S$$

This holds by Prop 2.4.3. □

Corollary 11.6 (2.7.8). *Let*

$$\begin{aligned} A^r &\xrightarrow{\varphi} A^s \xrightarrow{\pi} M \rightarrow 0 \\ A^p &\xrightarrow{\psi} A^q \xrightarrow{\lambda} N \rightarrow 0 \end{aligned}$$

be presentations of A -modules, then

$$A^{sp+rq} = (A^s \otimes_A A^p) \oplus (A^r \otimes_A A^q) \xrightarrow{\sigma} A^{sq} = A^s \otimes_A A^q \xrightarrow{\pi \otimes \lambda} M \otimes_A N \rightarrow 0$$

is exact where....

σ is the composition of $(\text{id}_{A^s} \otimes \psi) \oplus (\varphi \otimes \text{id}_{A^q})$ and $A^{sq} \oplus A^{sq} \xrightarrow{\pm} A^{sq}$ with $(x, y) \mapsto x + y$.

Proof. Uses Theorem 2.7.6. □

Instead of giving the proof, let's unravel it in a matrix example.

Example 11.7. $r = 3, s = 2, p = 1, q = 3$. Then $sq = 6$ and $sp + rq = 2 + 9 = 11$.

$$\varphi = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}, \quad \psi = \begin{bmatrix} u \\ v \\ w \end{bmatrix}$$

Then

$$\text{id}_{A^2} \otimes \psi = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} u \\ v \\ w \end{bmatrix} = \begin{bmatrix} uu & 0 \\ v & 0 \\ w & 0 \\ 0 & u \\ 0 & v \\ 0 & w \end{bmatrix}$$

and

$$\varphi \otimes \text{id}_{A^3} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \otimes I_{3 \times 3} = \begin{bmatrix} aI_{3 \times 3} & bI_{3 \times 3} & cI_{3 \times 3} \\ dI_{3 \times 3} & eI_{3 \times 3} & fI_{3 \times 3} \end{bmatrix}$$

with

$$\sigma^+ \circ (\text{id} \otimes \psi \oplus \varphi \otimes \text{id}) = \begin{bmatrix} I_6 & I_6 \end{bmatrix} \circ \begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$$

which gives

$$= \begin{matrix} e_1 \otimes f_1 \\ e_1 \otimes f_k \\ \vdots \\ e_2 \otimes f_3 \end{matrix} \begin{bmatrix} u & 0 & & & \\ v & 0 & aI_{3 \times 3} & bI_{3 \times 3} & cI_{3 \times 3} \\ w & 0 & & & \\ 0 & u & & & \\ 0 & v & dI_{3 \times 3} & eI_{3 \times 3} & fI_{3 \times 3} \\ 0 & w & & & \end{bmatrix}$$

Prop 2.7.10 characterizes relations in $M \otimes N$.

Proposition 11.8 (2.7.11). *If B, C are A -algebras, then $B \otimes_A C$ is an A -algebra, which is characterized by the following universal property for any commutative diagram of A -algebras (insert diagram with counterclockwise block diagram $\beta, \alpha : C, B \rightarrow D$ and $i, j : A \rightarrow C, B$). Then there exists a unique A -algebra homomorphism $\lambda : B \otimes_A C \rightarrow D$ such that the diagram*

(get diagram from Anne or Tony)

commutes, with $\psi : c \mapsto 1 \otimes c$, $\varphi : b \mapsto b \otimes 1$.

Corollary 11.9 (2.7.13). *If $B = A[x_1, \dots, x_n]/I$ and $C = A[y_1, \dots, y_m]/J$, then $B \otimes_A C = A[x_1, \dots, x_n, y_1, \dots, y_m]/\langle I, J \rangle$.*

Fiber product of algebraic varieties: (get diagram from Tony)

April 4

April 6

11.1 Integral Closure (3.2)

$I \subset A$ an ideal, $A \subset B$ rings. An element $b \in B$ is *integral* over I if $b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n = 0$ for some $a_i \in I$. If $a_i \in I^i$, then b is *strongly integral* over I .

$$C(I, B) := \{b \in B \mid b \text{ is integral over } I\} \supseteq C_S(I, B) = \{b \in B \mid \dots \text{ strongly} \dots\}$$

Proposition 11.10 (3.2.2). *A Noetherian, S multiplicatively closed.*

1. $C(A, B)$ is a subring of B containing A and $C(I, B)$ is an ideal in $C(A, B)$.
2. $S^{-1}C(A, B) = C(S^{-1}A, S^{-1}B)$
3. $I \cdot C(A, B) \subseteq C_S(I, B) = \sqrt{I \cdot C(A, B)}$

Conclusion: IF $C(A, B)$ is computable and radicals are computable (Sec 4.3), then $C(I, B)$ is computable.

Let A be a reduced ring and $Q(A)$ its total ring of fractions. The *normalization* of A is the ring $\bar{A} = C(A, Q(A))$.

Proposition 11.11 (3.2.5). *For a Noetherian ring A , the following are equivalent:*

1. A is normal (i.e. $A = \bar{A}$).
2. A_P is normal for all prime ideals $P \subset A$
3. A_M is normal for all maximal ideals.

Example 11.12. $K[x_1, \dots, x_n]$ is normal Every rational function that satisfies a monic equation with polynomial coefficients is a polynomial.

Example 11.13. $\frac{K[x, y]}{\langle x^3 - y^2 \rangle} = K[t^2, t^3] \overset{\varphi}{\subset} \overline{K[t^2, t^3]} = K[t]$ which is just a line. So φ^* takes a line to a cusp.

Normalization and integral domain in Singular (Ex 3.2.3)

$$A = \mathbb{Q}[x, y, z] / \langle x^6 - x^3z - y^2z \rangle, I = \langle y \rangle$$

Then

$$\bar{A} \mathbb{Q}[t_1, t_2, t_3, t_4] / \langle t_2t_3 - t_1t_4, t_1^5 + t_1^2t_3 - t_2t_4, t_1^4t_3 + t_1t_3^2 - t_4^2 \rangle$$

with $\varphi : A \rightarrow \bar{A}$ and $(x, y, z) \mapsto (t_1, t_2, t_3), t_4 = \frac{yz}{x}$. $C(I, Q(A)) = \sqrt{I\bar{A}} = \sqrt{\langle \text{stuff}, t_2 \rangle} = \langle t_2, t_4, t_1^4 + t_1t_3 \rangle$. Geometric meaning? Algorithm (3.6), Hironaka?

Theorem 11.14 (“going down”). [3.2.9] *Let $A \subset B$ be Noetherian integral domains, A normal, B integral over A . Let $Q \subset B$ be a prime ideal, $P = Q \cap A$, and $P' \subset P$ a prime ideal in A . Then there exists a prime ideal $Q' \subset Q$ in B such that $Q' \cap A = P'$.*

Let’s do an example where this fails, i.e. where you need this hypothesis.

Example 11.15 (3.2.11). $A = K[y, z] \subset B = K[x, y, z] / (\langle x, y \rangle \cap \langle x + z \rangle)$. Now A is normal, B is integral over A , but the “going down” property fails for $Q = \langle x, y \rangle$ and take $P' = \langle 0 \rangle$. Does there exist a $Q' \subset Q$ satisfying $Q' \cap A = \langle 0 \rangle$?

11.2 Dimension (3.3)

$$\mathcal{C}(A) = \{ (P_0 \subset P_1 \subset \dots \subset P_m \subset A) : P_i \text{ prime} \}$$

all chains of prime ideals in a ring A .

The (Krull) dimension of A is

$$\dim(A) := \sup \{ \text{length}(P_0) : P_0 \in \mathcal{C}(A) \}$$

For a prime $P \subset A$, the *height* (“codimension”)

$$ht(P) = \sup \{ m \mid (P_0 \subset P_1 \subset \dots \subset P_m = P) \in \mathcal{C}(A) \}$$

For $I \subset A$, any ideal,

$$ht(I) := \inf \{ ht(P) \mid P \supseteq I \text{ prime} \}$$

Call $\dim(I) = \dim(A/I)$ the dimension of I .

Example 11.16. In Sec 3.5, we'll prove that all maximal chains of prime ideals in $K[x_1, \dots, x_n]$ have the same length $n \implies \dim(K[x_1, \dots, x_n]) = n$. In the above example 3.2.11, $\dim(A) = \dim(B) = 2$.

Corollary 11.17 (3.3.3). *Let $A \subset B$ be an integral extension. Then $Q \mapsto Q \cap A$ determines a surjection from chains in B to chains in A ($\mathcal{C}(B) \rightarrow \mathcal{C}(A)$) preserving the length of chains. In particular, $\dim(A) = \dim(B)$.*

Proof. By Proposition 3.1.10, ("lying over") the map $Q \mapsto Q \cap A$ is surjective. We must prove that the length of chains is preserved. What do we mean by that? Say we have a chain in B . The problem is that if Q is strictly contained in some other Q' , then when you restrict, you still have Q . Suppose not, and let $Q \subset Q'$ be primes in B which have the same intersection in A , $Q \cap A = Q' \cap A =: P$. Then we localize, so $A_P \subset B_P$. Then $A_P \subset B_P$ is integral and (A_P, PA_P) is local. The ideals $QB_P \subseteq Q'B_P$ are prime in B_P , and $QB_P \cap A_P = Q'B_P \cap A_P = PA_P$. By Lemma 3.1.9 (3), QB_P and $Q'B_P$ are maximal and hence equal. (if something is a field over there, then it must be a field over here). This implies $Q = Q'$. \square

Think about B_P as taking the localization on $A \setminus P$ and then pushing that forward.

Definition 11.18 (3.3.4). A ring, $I \subset A$ ideal. A prime P is a *minimal (associated) prime* of I if $I \subset P$ and P is minimal with this property. The set of all minimal primes is denoted $\text{minAss}(P)$.

Example 11.19 (3.3.8). `> ring A=0,(x,y,z),dp;`

```
> ideal I=xz,yz;
> LIB "primdec.lib";
// ** loaded /usr/local/Singular/2-0-3/LIB/primdec.lib (1.98.2.10,2002/03/25)
// ** loaded /usr/local/Singular/2-0-3/LIB/matrix.lib (1.26.2.1,2002/02/20)
// ** loaded /usr/local/Singular/2-0-3/LIB/ring.lib (1.17.2.1,2002/02/20)
// ** loaded /usr/local/Singular/2-0-3/LIB/inout.lib (1.21.2.3,2002/02/20)
// ** loaded /usr/local/Singular/2-0-3/LIB/random.lib (1.16.2.1,2002/02/20)
// ** loaded /usr/local/Singular/2-0-3/LIB/poly.lib (1.33.2.5,2002/04/09)
// ** loaded /usr/local/Singular/2-0-3/LIB/elim.lib (1.14.2.2,2002/02/20)
// ** loaded /usr/local/Singular/2-0-3/LIB/general.lib (1.38.2.7,2002/04/12)
> minAssGTZ(I);
[1]:
  _[1]=z
[2]:
  _[1]=y
  _[2]=x
```

$$\begin{bmatrix} a & b & c & d & e \\ f & g & h & i & j \end{bmatrix}$$

$$I = \langle ag - bf, bh - cg, ci - dh, dj - ei \rangle$$

```
> ring B=0,(a,b,c,d,e,f,g,h,i,j),dp;
> ideal I = ag-bf, bh-cg,ci-dh,dj-ei ;
> minAssGTZ(I);
[1]:
  _[1]=-ei+dj
```

```

    _[2]=-eh+cj
    _[3]=-dh+ci
    _[4]=-eg+bj
    _[5]=-dg+bi
    _[6]=-cg+bh
    _[7]=-ef+aj
    _[8]=-df+ai
    _[9]=-cf+ah
    _[10]=-bf+ag
[2]:
    _[1]=g
    _[2]=-ei+dj
    _[3]=-eh+cj
    _[4]=-dh+ci
    _[5]=b
[3]:
    _[1]=h
    _[2]=-ei+dj
    _[3]=c
    _[4]=-bf+ag
[4]:
    _[1]=i
    _[2]=d
    _[3]=-cg+bh
    _[4]=-cf+ah
    _[5]=-bf+ag
[5]:
    _[1]=i
    _[2]=g
    _[3]=d
    _[4]=b

```

April 11

Proposition 11.20 (3.3.5). *Let A be a Noetherian ring and $I \subset A$ any ideal. Then $\text{minAss}(I) = \{P_1, \dots, P_n\}$ is finite and $\sqrt{I} = P_1 \cap \dots \cap P_n$. In particular, \sqrt{I} is the intersection of all primes containing I .*

Lemma 11.21 (3.3.6). *If $I : \langle a \rangle = I : \langle a^2 \rangle$ then $I = (I : \langle a \rangle) \cap \langle I, a \rangle$.*

Example 11.22. A case where this equation doesn't hold. $I = \langle 12 \rangle \subset A = \mathbb{Z}$, $a = 2$, then $(I : \langle a \rangle) = \langle 6 \rangle$, which is $\langle 6 \rangle \cap \langle 2 \rangle = \langle 6 \rangle$ and $\langle I, a \rangle = \langle 2 \rangle$ but this is strictly $\supset I$.

Geometrically, I gives some variety. And the name of the game is to break this variety into so many pieces. What's the role A plays in this progress. We want to find a hypersurface A that contains some of the pieces.

Lemma 3.3.6. Let $f \in (I : \langle a \rangle) \cap \langle I, a \rangle$ and write $f = g + xa$ for some $g \in I$. Then $af = ag + xa^2 \in I \implies xa^2 \in I \implies x \in (I : \langle a^2 \rangle) = (I : \langle a \rangle) \implies ax \in I \implies f \in I$. \square

So the proof is pretty straightforward but it's key to recognize that the hypothesis is exactly what we need.

Proposition 3.3.5. Since $\min\text{Ass}(I) = \min\text{Ass}(\sqrt{I})$, we may assume that $I = \sqrt{I}$. If I is prime, then we're done. Otherwise, $\exists a, b \notin I$, but $ab \in I$.

Claim: $\sqrt{I : \langle a \rangle} = I : \langle a \rangle = I : \langle a^2 \rangle \supset I$.

The containment is strict because of b . The second equality holds because I is radical. This means that $fa^2 \in I$, which gives that $(fa)^2 \in I \implies fa \in I$. The same reasoning works for the first equality. This means that $f^p \cdot a \in I$, which gives $(fa)^p \in I \implies fa \in I$.

By Lemma 3.3.6, $I = (I : \langle a \rangle) \cap \sqrt{\langle I, a \rangle}$ and both ideals are strictly bigger. Now we do this thing called Noetherian induction. So we continue (using Noetherianity) to get $I = P_1 \cap \dots \cap P_n$, P_i prime ideals, and $P_i \not\subseteq P_j$.

Claim: $\min\text{Ass}(I) = \{P_1, P_2, \dots, P_n\}$.

Suppose $P \supset \bigcap_{i=1}^n P_i$, then this implies that $\exists i$ such that $P \supseteq P_i$ by Lemma 1.3.12. \square

One way to compute \sqrt{I} from I :

- compute $\min\text{Ass}(I) = \{P_1, \dots, P_n\}$
- intersect these primes

Now suppose that

- $I = \langle f \rangle$, $\sqrt{I} = \langle \text{square-free part of } f \rangle$. A faster way would be to do $\frac{f}{\gcd(f, f')}$.
- $I = \langle \text{monomial ideal} \rangle$, then \sqrt{I} is gotten by erasing the exponents.

This brings us to the following question:

Q: When passing from $I \subset K[x_1, \dots, x_n]$ to \sqrt{I} , can the degrees of the generators ever increase?

A: Yes. Take $A = \mathbb{Q} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$, and take $I = \langle \text{all } 2 \times 2\text{-subpermanents} \rangle = \langle ae + bd, af + cd, \dots \rangle$.

$\min\text{Ass}(I)$ consists of 15 primes of height 6: six like $\langle a, b, c, d, e, f \rangle$ and 9 like $\langle ae + bd, c, f, g, h, i \rangle$. So the intersection is $\sqrt{I} = I + \langle aei \rangle$. By Nakayama's, while generators of an ideal are not unique, the betti numbers are (in a graded or local situation), so you can't go wrong with your choices. See the paper by D. Eisenbud and B. Sturmfels on "Binomial Ideals", the "baby bear" of the three bears.

Q: How to compute dimension in practice?

A: Use (square-free) monomial ideals (Chap 5). To make the next part true, need to tie in the notion of Krull dimension and the Hilbert polynomial.

$$\dim(K[x_1, \dots, x_n]/I) = \dim(K[x_1, \dots, x_n]/L(I)) = \dim(K[x_1, \dots, x_n]/\sqrt{L(I)})$$

Exercise: $I = \langle ab, bc, cd, de \rangle \subset \mathbb{Q}[a, b, c, d, e]$. What is $\dim(I)$, $\min\text{Ass}(I)$?

$\min\text{Ass}(I) = \{\langle b, d \rangle, \langle b, c, e \rangle, \langle a, c, e \rangle, \langle a, c, d \rangle\}$. In \mathbb{P}^4 , the variety looks like a house with the roof being a, c, e .

Theorem 11.23 (Noether Normalization 3.4.1). *Let K be a field, and $I \subset K[x_1, \dots, x_n]$. There exists an integer $s \leq n$ and an isomorphism $\varphi : K[x_1, \dots, x_n] \rightarrow K[y_1, \dots, y_n] =: A$ such that the following good things happen:*

1. *the map $K[y_{s+1}, \dots, y_n] \rightarrow A/\varphi(I)$ with $y_i \mapsto y_i \pmod{\varphi(I)}$ is injective and finite ($A/\varphi(I)$ is finitely generated as a module over the image)*
2. *φ can be chosen such that there exists polynomials*

$$g_j = y_j^{e_j} + \sum_{k=0}^{e_j-1} \xi_{j,k}(y_{s+1}, \dots, y_n) \cdot y_j^k \in \varphi(I)$$

satisfying $e_j \geq \deg(\xi_{j,k}) + k$ for $k = 0, \dots, e_j - 1$. (This enhances the module finiteness postulated in the previous statement. We're qualifying the shape that this integral relation takes. We can choose the integral relation so the later y 's are higher, using a degree lexi ordering.)

3. *If I is a homogeneous ideal, (such as in the exercise), then we can take the g_j to be homogenous (in the usual \mathbb{Z} -grading). If I is a prime ideal, (which isn't the above case), then we can take the g_j to irreducible.*
4. *If K is a perfect field (?), then φ can be chosen such that*

$$Q(A/\varphi(I)) \supset Q(K[y_{s+1}, \dots, y_n])$$

is a separable (?) field extention (provided that I is prime). (Note that this statement is void in the case of an infinite field of characteristic 0). Moreover, if K is infinite, then

$$Q(A/\varphi(I)) = Q(K[y_{s+1}, \dots, y_n])[y_s]/\langle g_s \rangle$$

5. *If K is infinite, then φ can be chosen to be linear, i.e $\varphi(x_i) = \sum_{j=1}^n m_{ij}y_j$ with $M = (m_{ij}) \in GL(n, K)$.*

This data is a Noether normalization of I .

What are good choices for s and φ in the previous exercise?

April 13

We'll start by proving the Theorem from last time called Noether normalization. It's a very important tool. If you can avoid doing this, it's better, because you really don't want to have to make a linear change of coordinates - this will change the structure of the original problem.

Proof. Suppose K is an infinite field. Use induction on n . (The freedom you have in a finite field in choosing the m_{ij} 's, you slip into the exponent).

$n = 1$: $I = \langle 0 \rangle$, trivial $s = 0$. If $I = \langle f \rangle \implies K[x]/\langle f \rangle \supset K$ is finite, so take $\varphi = \text{id}$. $s = 1$.

≥ 2 : Pick a polynomial $f \in I$ of positive degree d . (if there's a homogeneous polynomial, we'll use that one). Write it uniquely as a sum of homogeneous components:

$$f = f_d + f_{d-1} + \dots + f_1 + f_0$$

Consider a matrix $M_1 = (m_{ij}) \in \text{GL}_n(K)$ and $\bar{x} = M_1 \bar{y}$. This implies $f(\bar{x}) = f_d(m_{11}, \dots, m_{n1}) \cdot y_1^d +$ lower terms in y_1 . We can pick M_1 such that the leading coefficient $f_d(m_{11}, \dots, m_{n1})$ is non-zero. (It's very important to realize that it only depends on the first column of M_1). If we look at the rest of the variables in \bar{y} ,

$$K[y_2, \dots, y_n] \rightarrow A/\langle f \rangle \text{ is injective and finite}$$

and $\tilde{g}_1 = f(M_1 y)$ satisfies (2),(3). Now, writing I for $I\varphi(I)$, the map

$$K[y_2, \dots, y_n] / \underbrace{(I \cap K[y_2, \dots, y_n])}_{I_0} \rightarrow A/I \text{ is injective and still finite}$$

If $I_0 = \langle 0 \rangle$, we're done. Otherwise, by induction, \exists a matrix M_0 of format $(n-1) \times (n-1)$ such that

$$M_0 \begin{pmatrix} z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} y_2 \\ \vdots \\ y_n \end{pmatrix}$$

and for some s , the map

$$K[z_{s+1}, \dots, z_n] \rightarrow K[y_2, \dots, y_n]/I_0 \text{ is injective and finite, etc.}$$

Hence $K[z_{s+1}, \dots, z_n] \rightarrow A/I$ is finite and injective with transformation matrix

$$M = M_1 \cdot \begin{pmatrix} I & 0 \cdots 0 \\ \vdots & M_2 \end{pmatrix}$$

□

Algorithm 11.24 (3.4.5). **Input:** $I = \langle f_1, \dots, f_m \rangle \subset K[\bar{x}]$, $\bar{x} = (x_1, \dots, x_n)$.

Output: A set of variables $\{x_{s+1}, \dots, x_n\}$ and $\varphi: K[\bar{x}] \rightarrow K[\bar{x}]$ such that

$$K[x_{s+1}, \dots, x_n] \rightarrow K[\bar{x}]/\varphi(I) \text{ is a Noether normalization}$$

- Perform a random lower triangular coordinate change:

$$\varphi(x) = \begin{pmatrix} 1 & 0 \cdots 0 & 0 \\ & \ddots & \vdots \\ * & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

- Compute a reduced Gröebner basis $\{g_1, \dots, g_r\}$ of $\varphi(I)$ with respect to $x_1 > x_2 > \dots > x_n$ lex [and order the Gröebner basis such that $\text{LM}(g_1) < \dots < \text{LM}(g_r)$]
- Choose s minimal such that $\{g_1, \dots, g_r\} \cap K[x_{s+1}, \dots, x_n] = \emptyset$.
- For $i = 1, \dots, s$, test whether $\{g_1, \dots, g_r\}$ contains polynomials with leading monomials $x_1^{\rho_i}$ for some ρ_i
- If the test is true, then return φ and $\{x_{s+1}, \dots, x_n\}$
- Otherwise: Try Again.

11.3 Applications (3.5)

Theorem 11.25 (3.5.1). *Let K be a field, $A = K[x_1, \dots, x_n]$. Then the following holds:*

1. $\dim(A) = n$, moreover, all maximal chains in $\mathcal{C}(A)$ have length n
2. If $f \in A$, $\deg(f) \geq 1$ then $\dim(A/\langle f \rangle) = n - 1$ [Krull's Principle Ideal Theorem]
3. If P is any prime ideal, then $\text{ht}(P) + \dim(A/P) = n$.
4. If P is any prime ideal, then $\dim(A/P) = \text{trdeg}_K(Q(A/P))$ (where trdeg is the transcendence degree). Moreover, all maximal chains in $\mathcal{C}(A/P)$ have same length $\dim(A/P)$
5. If $M \subset A$ is a maximal ideal then $A/M \supset K$ is finite. (Nullstellensatz)
6. Let $I \subset A$ be any ideal and let $U \subseteq X$ such that $K[u] \cap I = \{0\}$. Then $\dim(A/I) \geq \#u$, and this bound is tight.

There are two more parts in the book.

Proof. Use induction on n , the case $n = 0$ being trivial.

1. Let $\langle 0 \rangle = P_0 \subset \dots \subset P_m \subset A$ be a maximal chain in $\mathcal{C}(A)$. (m finite by Noetherianity). Choose an irreducible $f \in P_1$ and coordinates y_1, \dots, y_{n-1} such that $K[x_1, \dots, x_n]/\langle f \rangle \supset K[y_1, \dots, y_{n-1}]$ is finite. Then the induced chain $\langle 0 \rangle = P_1/\langle f \rangle \subset P_2/\langle f \rangle \subset \dots \subset P_m/\langle f \rangle$ is maximal too. (we need all the lying over, going under, etc. theorems to make sure nothing slips in). This chain again induces (by Lemma 3.3.14) a maximal chain in $K[y_1, \dots, y_{n-1}]$, which by induction hypothesis has length $n - 1$. (note that P_1 has to be principle and generated by f).
2. immediate from proof of (1)
3. immediate from statement of (1)
4. We may assume $A/P \supset K[y_1, \dots, y_s]$ is finite. (using Noether normalization here) Corollary 3.3.3 $\implies \dim(A/P) = \dim(K[y_1, \dots, y_s]) \stackrel{(1)}{=} s$. (here we see that Noether normalization ensures that you're in a plane in the right position). But $\text{trdeg}_K Q(A/P) = \text{trdeg}_K K(y_1, \dots, y_s) = s$
5. (Really pay attention here because we prove the Nullstellensatz) (Aside: consider $(\overline{\mathbb{F}})^2$ which is a dynamical system (Frobenius) and thus has a zeta function) This is a consequence of of NNT (3.4.1) and the fact that M is maximal $K[y_1, \dots, y_x] \subset A/M$ is finite. Using Lemma 3.1.9 implies that $K[y_1, \dots, y_s]$ is a field $\implies s = 0$.
6. just read the book...(7) and (8) also.

□

Think about the primary decomposition of $I = \langle x^{243} - x, y^{243} - y \rangle$ for $\mathbb{F}_{243}^2 \subset (\overline{\mathbb{F}_7})^2$.

Now for a bit of rambling,...

$$\Delta_I := \{y \subseteq x | K[u] \cap I = \{0\}\}$$

is a family of independent sets. If $I = \langle a, b, c \rangle \subset K[a, b, c]$. What is Δ_I ?

$$\Delta_I = \{ab, ac, bc, a, b, c, \emptyset\}$$

is a *simplicial complex* of independent sets! So we can draw the picture as the boundary of a triangle. Now an equivalent statement of (6) is:

If $I \subset A$ is an ideal, $\dim(A/I) = \dim(\Delta_I) + 1$, where $\dim(\Delta_I) := \max\{\#u : u \in D_I\} - 1$. Think about the variety of I as being a line in the projective space.

Now take $I = \langle a + b + c, b + c + d \rangle \subset K[a, b, c, d]$. Draw Δ_I ? It's just a box with one diagonal between c and b (not a and d !)

April 20

Theorem 11.26 (Nullstellensatz (Zero Place theorem) (3.5.2)). *Let K be an algebraically closed field, $I \subset K[x_1, \dots, x_n]$ an ideal, and its variety*

$$V(I) = \{u \in K^n \mid f(u) = 0 \forall f \in I\}$$

If a polynomial $g \in K[\bar{x}]$ satisfies $g(u) = 0 \forall u \in V(I)$ then $g \in \sqrt{I}$.

Proof. Consider the ideal $J = \langle I, 1 - tg \rangle \in K[\bar{x}, t]$.

Case 1: ($1 \in \mathcal{J}$) $\implies \exists g_1, \dots, g_s \in I, h, h_1, \dots, h_s \in K[\bar{x}, t], 1 = \sum_{i=1}^s h_i g_i + h(1 - tg)$. Replace t by $\frac{1}{g}$ we find

$$1 = \sum_{i=1}^s g_i(x) \cdot h_i \left(\bar{x}, \frac{1}{g(x)} \right) \in K[\bar{x}]g$$

Clearing denominators, we find $g(x)^p \in \langle g_1, \dots, g_s \rangle \subseteq I$ for some $p > 0$.

Case 2: ($1 \notin \mathcal{J}$) Choose a maximal ideal $M \subset K[\bar{x}, t]$ such that $\mathcal{J} \subseteq M$. By Theorem 3.5.1 (5), $K[\bar{x}, t]/M$ is an algebraic extension of K . Then $(K = \bar{K}) \implies K[\bar{x}, t]/M \simeq K$ because K is algebraically closed, so $\implies M = \langle x_1 - u_1, \dots, x_n - u_n, t - u \rangle$ for some $u_1, u \in K$. Now we're using the fact that $\mathcal{J} \subseteq M$ which implies $(u_1, \dots, u_n, u) \in V(\mathcal{J})$ so $(I \subseteq \mathcal{J}) \implies (u_1, \dots, u) \in V(I)$. Now the g

has to vanish somewhere, so the hypothesis implies $g(u_1, \dots, u_n) = 0 \implies 1 - u \cdot g(u_1, \dots, u_n) = \begin{cases} 0 \\ 1 \end{cases}$
 Contradiction. □

Corollary 11.27. *For an ideal $I \subset K[x_1, \dots, x_n]$, the following are equivalent:*

1. $V(I) = \emptyset$
2. $1 \in I$
3. *The reduced Gröbner basis (w.r.t. any term order) equals $\{1\}$.*

This is kind of a duality theorem. If you have a system of polynomial equations with a point, or there exists a dual solution which are the multipliers. Clearly the case in Optimization theorem: either dual or primal solution. Is there possibly a generalization then? (i.e. other Nullstellensatz?)

- Real NS (a system of polynomial equations, either a solution over \mathbb{R} or there's a condition)

- Effective NS (system, one in the ideal, so we'd like to bound the degree, \exists multipliers with $\sum g_i f_i = 1$ and we want to bound the g_i 's)
- Arithmetic NS (give the $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$)
- ...

Independent Sets:

Definition 11.28 (3.5.3). Fix an ideal $I \subset K[x_1, \dots, x_n]$. A subset $U \subseteq \{x_1, \dots, x_n\}$ is an *independent set* if $K[U] \cap I = \{0\}$. We write Δ_I for the *simplicial complex* of independent sets (i.e. if $U \in \Delta_I$ and $V \subseteq U$, then $V \in \Delta_I$). If $U \in \Delta_I$ is maximal w.r.t. inclusion then U is called a *facet* of Δ_I . We represent Δ_I by listing all facets.

For I monomial ideal, $\Delta_I = V(I)$ is called the Stanley-Reisner complex. Also, recall $\dim(\Delta_I) = \dim(K[\bar{x}]/I) - 1$. Actually, $\Delta_{L(I)} \subseteq \Delta_I$ and they have the same dimension. Recall that the Krull dimension mod an ideal is the same mod any leading ideal with respect to any ordering. Then $\cup_{>} \Delta_{L_{>}(I)} = \Delta_I$.

insert table

Now $\langle ac, ad, bd \rangle = \langle a, b \rangle \cap \langle a, d \rangle \cap \langle c, d \rangle$ and $V(\langle ac, ad, bd \rangle) = V(\langle c, d \rangle) \cup V(a, d) \cup V(a, b)$. Now for a "real" question. What is Δ_I where $I = \langle 2 \times 2 \text{ minors of } 3 \times 3 \text{ matrix in } 9 \text{ variables} \rangle$. This is the Segre variety. $\mathbb{P}^2 \times \mathbb{P}^2 \subset \mathbb{P}^8$. Then $\Delta_I =$ the *matroid* of triangle \times triangle.

insert picture

An *algebraic matroid* is a simplicial complex of the form Δ_I where I is a *prime ideal* in $K[x_1, \dots, x_n]$. Please study these!!!

Finiteness of Normalization (E. Noether):

Theorem 11.29 (3.5.10). Let $A = K[x_1, \dots, x_n]/P$ where P is a prime ideal. Then the normalization \bar{A} is a finite A -module.

Note that this is false for arbitrary Noetherian integral domains - proved by Nagata.

Proof. Suppose K is perfect. (Every field of characteristic p has a p th root). Use Noether normalization to choose coordinates, y_1, \dots, y_s such that

$$K[y_1, \dots, y_s] \xrightarrow{\text{finite}} K[x_1, \dots, x_n]/P \hookrightarrow \bar{A}$$

but also

$$K[y_1, \dots, y_s] \hookrightarrow K(y_1, \dots, y_s) \xrightarrow{\text{finite and separable}} Q(K[x_1, \dots, x_n]/P) \supset \bar{A}$$

\bar{A} is also the integral closure of $K[y_1, \dots, y_s]$ in $Q(K[x_1, \dots, x_n]/P)$. Since $K[y_1, \dots, y_s]$ is a normal Noetherian domain, (and integrally closed in its own field of fractions), it suffices to prove the following lemma:

Lemma 11.30 (3.5.12). *Let A be a NND, $L \supset Q(A)$ a finite separable field extension, and B the integral closure of A in L . Let $\alpha \in B$ be a primitive element of this field extension, F the minimal polynomial with $\deg(F) = d$, and Δ the discriminant of F . Then $B \subseteq \frac{1}{\Delta}A[\alpha] = \frac{1}{\Delta}A\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$. In particular, B is finite as an A -module.*

We'll finish with an example and prove this next time..... □

Example 11.31. $n = 4$. $P = \langle bc - ad, c^3 - bd^2, ac^2 - b^2d, b^3 - a^c \rangle$, $k[a, b, c, d]/P \simeq K[s^4, s^3t, st^3, t^4]$, $A = K[a, d] = K[s^4, t^4]$, with $Q(A) = K(a, d)$. The questions are the following:

- $L = Q(K[a, b, c, d]/P) = ?$
- $L \supset Q(A)$ is an algebraic extension of degree = ?
- $\alpha, F, \Delta = ?$

April 25

Theorem 11.32 (4.1.4). *Let A be a Noetherian ring, I an ideal. Then there exists an irredundant decomposition into primary ideals, $I = Q_1 \cap \dots \cap Q_r$.*

Proof. By Lemma 4.1.3(2) □

Theorem 11.33 (4.1.5). *Let A be a ring, $I \subset A$ an ideal with an irredundant primary decomposition $I = Q_1 \cap \dots \cap Q_r$. Then $r = \#\text{Ass}(I)$ and $\text{Ass}(I) = \{\sqrt{Q_1}, \dots, \sqrt{Q_r}\}$. If $\text{Ass}(I, P) = \{\sqrt{Q_{i_1}}, \dots, \sqrt{Q_{i_s}}\}$ for $P \in \text{Ass}(I)$, then $Q_{i_1} \cap \dots \cap Q_{i_s}$ is independent of the intersection.*

Proof. Suppose we have the decomposition in the hypothesis and $P \in \text{Ass}(I)$. Pick $b \in A$ such that $\bar{P} = I : \langle b \rangle \implies$ (Ex 4.1.3), $P = (Q_1 : \langle b \rangle) \cap \dots \cap (Q_r : \langle b \rangle)$. By Lemma 1.3.12, $\implies P = Q_j : \langle b \rangle$. By Lemma 4.1.3 (3), $Q_j : \langle b \rangle \subseteq \sqrt{Q_j} \implies P = \sqrt{Q_j}$.

We have shown $\{\sqrt{Q_1}, \dots, \sqrt{Q_r}\} \subseteq \text{Ass}(I)$. The converse is derived from Lemma 4.1.3... □

May 4

11.4 Higher-Dimensional Primary Decomposition (4.3)

Proposition 11.34 (4.3.1). *Let $I \subset K[\underbrace{x_1, \dots, x_n}_X]$ be any ideal and $U \in \Delta_I$ maximal w.r.t. cardinality. Then*

1. $I \cdot K(U)[X \setminus U]$ is a zero-dimensional ideal in $K(U)[X \setminus U]$
2. Let $G = \{g_1, \dots, g_r\} \subset I \subset K[X]$ be a Gröbner basis for $I \cdot K(U)[X \setminus U]$ and let $h := \text{lcm}(\underbrace{LC(g_1), \dots, LC(g_r)}_{\in K[U]})$. The $I \cdot K(U)[X \setminus U] \cap K[X] = I : \langle h^\infty \rangle$ (*) and this ideal is equidimensional of dimension $\dim(I)$.

3. Let $I \cdot K(U)[X \setminus U] = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition (computed on Thursday). Then

$$IK(U)[X \setminus U] \cap K[X] = (Q_1 \cap K[X]) \cap \cdots \cap (Q_s \cap K[X])$$

is an irredundant primary decomposition.

Proof. 1. Follow from Theorem 3.5.1 (6)

2. Obviously, $I : \langle h^\infty \rangle \subset I \cdot K(U)[X \setminus U] \cap K[X]$. To prove ' \supseteq ', let $f \in \text{RHS}$. Since G is a Gröbner basis, we have $f \xrightarrow{G} 0$. This reduction process in $K(U)[X \setminus U]$ shows that some power of h times f is in I , i.e. $h^m f \in I$ for some m . To show the second statement, $I : \langle h^\infty \rangle$ is equidimensional in $K[X]$ consider a irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_s$. Suppose $Q_i \cap K[U] = \langle 0 \rangle$ for $i = 1, \dots, r$ and \neq for $i = r + 1, \dots, s$. Since $U \in \text{Delta}_{Q_i}$ for $i = 1, \dots, r$ we have $\dim(Q_i) \geq \#U$. Since $\#U = \dim(I)$, we conclude $\dim(Q_i) = \dim(I)$ for $i = 1, \dots, r$.

Note: $I \cdot K(U)[X \setminus U] = \bigcap_{i=1}^r Q_i K(U)[X \setminus U]$ is a primary decomposition (by Exercise 4.3.3). Intersecting this primary decomposition with $K[x]$ we find that $I : \langle h^\infty \rangle = \bigcap_{i=1}^r Q_i$ is equidimensional.

(note that the Q_i notation is different from what we mean in part 4)

3. Easy to check $Q_i \cap K[X]$ is primary and $\sqrt{Q_i \cap K[X]} \neq \sqrt{Q_j \cap K[X]}$ for $i \neq j$. □

Algorithm 11.35 (Reduction to Zero (I) (4.3.2)). **Input:** $I = \langle f_1, \dots, f_k \rangle \subset K[X]$

Output: A triple (U, G, h) where

- U is a maximally independent set w.r.t I .
- $G = \{g_1, \dots, g_s\} \subset I$ is a GB of $I \cdot K(U)[X \setminus U]$
- $h \in K[U]$ such that $I \cdot K(U)[X \setminus U] = I : \langle h \rangle = I : \langle h^\infty \rangle$

Idea: Take G to be the purely lexicographical GB w.r.t. $X \setminus U > U$.

Algorithm 11.36 (Decomp(I) (4.3.4)). **Input:** $I = \langle f_1, \dots, f_k \rangle \subset K[X]$

Output: A set of pairs (Q_i, P_i) of ideals in $K[X]$ for $i = 1, \dots, r$ such that

- $I = Q_1 \cap \cdots \cap Q_r$ is a (possibly redundant) primary decomposition.
- $P_i = \sqrt{Q_i}$.

The steps are:

- $(U, G, h) := \text{Reduction to Zero(I)}$
- Change ring to $K(U)[X \setminus U]$ and compute $\text{qprimary} := \text{zerodecomp}(\langle G \rangle_{K(U)[X \setminus U]})$
- Change ring to $K[X]$ and compute

$$\text{primary} := \{(Q^1 \cap K[X], P^1 \cap K[X]) \mid (Q^1, P^1) \in \text{qprimary}\}$$

- `primary := primary ∪ decomp(⟨I, h⟩)`
- `return primary`

Note: $I = (I : h) \cap \langle I, h \rangle$, since $(I : h) = (I : h^2)$. Also, given any ideal \mathcal{J} in $K(U)[X \setminus U]$, how to compute $\mathcal{J} \cap K[X]$? Answer: Exercise 4.3.4 (page 258).

Example 11.37 (How to solve linear PDE's with constant coefficients). `> ring R=0,(d1,d2,d3,d4),dp;`

`> ideal I=d1*d3,d1*d4+d2*d3,d2*d4;`

`> LIB"primdec.lib";`

`> primdecGTZ(I);`

[1]:

[1]:

_ [1]=d4

_ [2]=d3

[2]:

_ [1]=d4

_ [2]=d3

[2]:

[1]:

_ [1]=d2

_ [2]=d1

[2]:

_ [1]=d2

_ [2]=d1

[3]:

[1]:

_ [1]=d4^2

_ [2]=d3*d4

_ [3]=d3^2

_ [4]=d2*d4

_ [5]=d2^2

_ [6]=d2*d3+d1*d4

_ [7]=d1*d3

_ [8]=d1*d2

_ [9]=d1^2

[2]:

_ [1]=d1

_ [2]=d2

_ [3]=d3

_ [4]=d4

Output: $\text{Ass}(I) = \{\langle d1, d2 \rangle, \langle d3, d4 \rangle, \langle d1, d2, d3, d4 \rangle\}$. This means in terms of PDE's:

$$\left(\lambda \frac{\partial}{\partial x_1} + \mu \frac{\partial}{\partial x_2} \right) \left(\lambda \frac{\partial}{\partial x_3} + \mu \frac{\partial}{\partial x_4} \right) f(x_1, x_2, x_3, x_4) = 0$$

for all $\lambda, \mu \in \mathbb{R}$. Also,

$$\frac{\partial^2}{\partial x_1 \partial x_3} = \frac{\partial^2}{\partial x_1 \partial x_4} + \frac{\partial^2}{\partial x_2 \partial x_3} = \frac{\partial^2}{\partial x_2 \partial x_4} = 0$$

$$f(\bar{x}) = A(x_3, x_4) + B(x_1, x_2) + \gamma \cdot \det \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

May 4

11.5 The Radical (4.5)

Proposition 11.38 (4.5.1). *Let $I \subset K[x_1, \dots, x_n]$ be a zero-dimensional ideal and $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, 2, \dots, n$. Moreover, let g_i be the squarefree part of f_i . Then*

$$\sqrt{I} = I + \langle g_1, \dots, g_n \rangle$$

Proof. Clearly, $I \subseteq I + \langle g_1, \dots, g_n \rangle \subseteq \sqrt{I}$. Need only show, $a^m \in I \implies a \in I + \langle g_1, \dots, g_n \rangle$. Each g_i is the product of distinct linear factors in $\bar{K}[x_i]$. By Exercise 4.17, these linear factors induce a splitting of

$$(I + \langle g_1, \dots, g_n \rangle) \bar{K}[\bar{x}]$$

into an intersection of maximal ideals. Hence it is radical. Now, if $a^m \in I$ then $a \in (I + \langle g_1, \dots, g_n \rangle) \bar{K}[\bar{x}] \cap K[\bar{x}] = I + \langle g_1, \dots, g_n \rangle$. \square

There is Algorithm 4.5.2 (`zeroideal(I)`), which does precisely this.

Reduction to the zero-dimensional case:

Let U be a maximal set in Δ_I . Pick $h \in K[U]$ such that $I \cdot K(U)[X \setminus U] \cap K[X] = I : \langle h \rangle = I : \langle h^\infty \rangle \implies I = (I : \langle h \rangle) \cap \langle I, h \rangle$. This implies that

$$\sqrt{I} = \underbrace{\sqrt{I : \langle h \rangle}}_{\sqrt{I \cdot K(U)[X \setminus U] \cap K[X]}} \cap \sqrt{\langle I, h \rangle}$$

Compute the left part using `zeroradical` and the right part by induction. This is all accomplished by Algorithm 4.5.3 (`radical(I)`).

Example 11.39.

$$\sqrt{\langle ac, ad + bc, bd \rangle} = \langle ac, ad, bc, bd \rangle = \langle a, b \rangle \cap \langle c, d \rangle$$

Q: $X = (x_{ij})$ a 3×3 -matrix of unknowns. What is $\sqrt{\langle \text{entries of } X^3 \rangle}$?

A: This is the set of all polynomials that vanish on the variety of all nilpotent 3×3 -matrices. But this is simply the coefficients of the characteristic polynomial, i.e. the trace, the determinant, and something of degree 2. This has dimension 6, but has height 3, i.e. strictly upper or lower triangular matrices which are nilpotent.

On Tuesday, we'll talk about the real numbers. How about computing the *real radical* of an ideal $I \subset \mathbb{R}[x_1, \dots, x_n]$?

$$\sqrt[\mathbb{R}]{I} := I(V_{\mathbb{R}}(I))$$

This is the Real Nullstellensatz. For example, consider $\sqrt[\mathbb{R}]{\langle x^3 + x \rangle} = \langle x \rangle$. We know the answer because we can factor it, and the variety of $x^2 + 1$ is non-empty because sums of squares in \mathbb{R} can never be negative, or zero.

11.6 Properties of the Hilbert Polynomials (5.3)

Let A be a graded K -algebra and M a finitely generated graded A -module and let

$$P_M(m) = \sum_{i=1}^d a_i m^i, \quad (a_d \neq 0)$$

be the *Hilbert polynomial* of M . Then set

$$d(M) := d = \deg(P_M)$$

Theorem 11.40 (5.3.7). *Let $I \subset K[x_1, \dots, x_n]$ be a homogeneous ideal. Then*

$$\dim(K[\bar{x}]/I) = d \left(\frac{K[\bar{x}]}{I} \right) + 1$$

Example 11.41. $n = 4$. $I = \langle x_1^2, x_2^2 \rangle$. This implies that

$$K[x_1, x_2, x_3, x_4]/I \simeq K[x_3, x_4] \oplus x_1 K[x_3, x_4] \oplus x_2 K[x_3, x_4] \oplus x_1 x_2 K[x_3, x_4]$$

Then $P_{K[\bar{x}]/I} = 4 \cdot m$ because $(m+1) + m + m + (m-1)$.

Idea of proof. Using Noether Normalization, $K[\bar{x}]/I$ can be written as a finitely generated graded $K[y_1, \dots, y_s]$ -module where $s = \dim(K[\bar{x}]/I)$. We have $\deg(P_{K[\bar{x}]/I}) = \deg(P_{K[\bar{y}]}) = s - 1$ with equality by Proposition 5.3.6. \square

12 Invariant Theory

This was Emil Noether's thesis topic published in 1907. Let G be a finite group acting linearly on $K[x_1, \dots, x_n]$ with $\text{char}(K) = 0$. The goal is to compute the subring $K[\bar{x}]^G$ of invariant polynomials. Consider the examples:

1. $K[x, y, z]^{S_3} = K[x + y + z, xy + xz + yz, xyz]$
2. $K[x, y, z]^{A_3} = K[x + y + z, xy + xz + yz, xyz, (x - y)x - z)y - z]$
3. $K[x, y, z]^{\mathbb{Z}^2} = K[x^2, xy, xz, y^2, yz, z^2]$

Theorem 12.1 (Hilbert). *G can be reductive here. $K[\bar{x}]^G = K[f_1, \dots, f_r]$ for some finite list of invariant polynomials f_i .*

Proof. So clearly, subalgebras are not finitely generated. But the basis theorem applies to ideals. So look at the following ideal $I = \langle K[\bar{x}]_+^G \rangle$ of homogeneous invariants of positive degree. I have no idea what they are but they'll generate some proper ideal. It's finitely generated, $I = \langle f_1, \dots, f_r \rangle$, called the *nullcone* in literature. We can assume that these polynomials are invariant, $f_i \in K[\bar{x}]^G$.

Claim: These f_i actually generate the algebra.

This is clearly not true in general, like $K[x, xy, xy^2, xy^3, \dots]$ and the ideal $\langle x \rangle$ doesn't work. So consider the *Reynolds operator*.

$$\rho : K[\bar{x}] \rightarrow K[\bar{x}]^G, \quad g \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \sigma \circ g = \int_{x \in G} g(x) d\mu(x)$$

where μ is the Haar measure. What's good about this operator is that fixes the invariants, $\rho(f_i) = f_i$. Let g be an invariant polynomial of positive degree. It must be in the ideal so

$$g = h_1 f_1 + h_2 f_2 + \cdots + h_r f_r \text{ for some } h_i \in K[\bar{x}]$$

where h_i are of degree strictly smaller than the degree of g . Now

$$\begin{aligned} g = \rho(g) &= \rho(h_1 f_1) + \cdots + \rho(h_r f_r) \\ &= \rho(h_1) f_1 + \cdots + \rho(h_r) f_r \end{aligned}$$

since the f_i are invariant. The goal is to show that $g \in K[f_1, \dots, f_r]$. But $\rho(h_i) \in K[f_1, \dots, f_r]$ and $h_r \in K[f_1, \dots, f_r]$. \square

Q: How do you actually compute f_1, \dots, f_r ? This is where Gröbner bases must be invented.

If you're interested in learning more, see *Computational Invariant Theory* by Derksen-Kemper.