- A primary decomposition $I = \bigcap_{i=1}^{n} Q_i$ is <u>irredundant</u> if $\forall j \in \{1, \dots, n\}$

$$\bigcap_{i \neq j} Q_i \neq I \qquad \text{(no extraneous factor)}$$

- By previous exercise we may assume that $\sqrt{Q_i} = P_i$ are all distincts. And then P_i's are called the associated primes of I
- An associated prime P_i which does not properly contain any other assoc. prime P_j is called a <u>minimal</u> assoc. prime
- The non-minimal associated prim are called <u>embedded</u> associated primes.

<u>Ex:</u> • $I_1 = (x^2, xy) = (x^2, y) \cap (x)$ ← both primary ideals

(x) ← minimal assoc. prim.

(x, y) ← embedded associated prim.

"$V(I \cap J) = V(I) \cup V(J)$" (ex.)

Notice that $I_1 = (x^2, xy, y^2) \cap (x)$ both primary.

<u>primary</u> <u>decomposition</u> is <u>not</u> <u>unique</u>. M2.

- Radical remove embedded components

(minimal primes → $\sqrt{I}$ is the intersection of the minimal primes of I.)

• $I_2 = (x) \cap (x-1, y) = (x^2 - x, xy)$ 2 minimal primes.

$f = xh = p(x-1) + q \cdot y \Rightarrow -p(0,y) + yq(0,y) = 0 \Rightarrow p(0,y) = yq(0,y)$

$\Rightarrow p = yq(0,y) + xp' \Rightarrow f = x(x-1)p' + q \cdot y + (x-1)yq(0,y) = x(x-1)p' + xy\,q(0,y) + \underbrace{q \cdot y - q(0,y) \cdot y}_{\text{divisible per } x}$

(N.B. Embedded primes are important $\to$ (theory of schemes
Grothendieck))

- Question: How to find associated primes and a primary decomposition?

Def: R ring. I, J ideals in R. $(I:J) = \{ f \in R : f.J \subseteq I \}$ is called the ideal quotient of I by J.

Lemma: If Q is P-primary and $f \in R$ then:

i) $f \in Q \Rightarrow Q:f = R$
ii) $f \notin Q \Rightarrow Q:f$ is P-primary
iii) $f \notin P \Rightarrow Q:f = Q$

Proof: i) clear iii) $g \in (Q:f) \Rightarrow g.f \in Q$ but $f^p \notin Q$ (otherwise $f \in P$).

ii) ~~$g.h \in (Q:f) \Rightarrow f.g.h \in Q \Rightarrow g^m.h^m \in Q$~~

If $g \in Q:f$ then $g^n \in Q$ because $f \notin Q$ and Q primary

(exercise)

this implies that $g \in \sqrt{Q} = P$. So we have

$$Q \subseteq (Q:f) \subseteq P \quad \text{and hence } \sqrt{(Q:f)} = P.$$

To show that $(Q:f)$ is primary, let $a.b \in (Q:f)$.

if $a \in (Q:f)$, then OK, otherwise $a \notin (Q:f)$, i.e. $fa \notin Q$.

but $a.b \in (Q:f) \Rightarrow (f.a).b \in Q \underset{Q \text{ primary}}{\Rightarrow} b^n \in Q \subseteq (Q:f)$

$\square$.

<u>Exercise</u>: (Distributivity)

1) If a prime ideal $P = I_1 \cap I_2$ then $P = I_1$ or $P = I_2$
2) Show that $(I_1 \cap I_2) : f = (I_1 : f) \cap (I_2 : f)$
3) $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$

(1) If $I_1 \cap I_2 \neq I_1$ and $\neq I_2$ then $\exists\, f_1 \in I_1$ and $f_2 \in I_2$ such that $f_1 \notin I_1 \cap I_2$, $f_2 \notin I_1 \cap I_2$, $f_1 \cdot f_2 \in I_1 \cap I_2$. So $I_1 \cap I_2$ is not prime.)

<u>Corollary</u>: The associated primes of an ideal are independent of the decomposition.

<u>Pf</u>: Let $I = \bigcap_{j=1}^{n} Q_j$ irredundant.

One can choose $f_i \notin Q_i$ but $f_i \in Q_j$ $\forall j \neq i$. so

$I : f_i = Q_i : f_i$ is P_i-primary. $P_i = \sqrt{Q_i : f_i}$

So the P_i's belong to the set $\{\sqrt{I : f} \mid f \in R\}$.

Now, if P is a prime of the form $\sqrt{I : f}$, for some f ??

$$P = \sqrt{(I : f)} = \sqrt{\bigcap_j (Q_j : f)} = \bigcap_j \sqrt{Q_j : f} = \bigcap_j P_j$$

$\Rightarrow$ $P = P_j$ for some j.

$\square$.

<u>Exercise</u>: Prove that $\sqrt{I}$ is the intersection of the minimal primes of I.

4) The Nullstellensatz and Zariski Topology.

Given varieties X, Y, it is natural to consider maps $f: X \to Y$. We need a topology.

Def: (topology) A top. on a set X is a collection $\mathcal{U}$ of subsets of X such that:

- $\emptyset$ and X are in $\mathcal{U}$
- $\mathcal{U}$ is closed under finite intersection
- $\mathcal{U}$ is —— arbitrary union

Members of $\mathcal{U}$ are called open sets. Closed sets are complement of open sets.

- Zariski topology:

$\mathbb{A}^n_k$: Closed sets in k^n are affine varieties $V(I)$ $I \subset k[x_1, \dots, x_n]$ (closed under finite union).

If X is a variety in k^n then X is equipped with the subspace topology (open set in X = open set in $k^n \cap X$)

"k will be most of the time alg. closed field."

- If $U = \complement V(f)$, $f \in R[x_1, \dots, x_n]$ then U is called a distinguished open set and denoted by U_f.

$\to$ Every Zariski open set can be written as a union of distinguished open sets.

- We have seen that $J \subseteq I(V(J))$ and that this could be a proper containment.

Notice that from the dif. of $\sqrt{J}$, we have $J \subseteq \sqrt{J} \subseteq I(V(J))$.

To get the precise relation between J and $I(V(J))$ we first consider this question:

when is the variety of an ideal empty?

- It is clear that if $1 \in I$ then $V(I) = \emptyset$
- On the other hand, $(x^2+1) \subseteq \mathbb{R}[x]$ is proper and $V_{\mathbb{R}}(x^2+1) = \emptyset$. But:

THM: If k is alg. closed field and $V(I)$ is empty then $1 \in I$.

(Hilbert) weak Nullstellensatz.

THM: (Strong Nullstellensatz) k alg. closed.

If $f \in I(V(J)) \subseteq k[x_1,\dots,x_n]$, then $f^m \in J$ for some m, i.e. $\sqrt{J} = I(V(J))$.

Pf: $J = (f_1,\dots,f_s)$ $\quad f \in I(V(J))$ $\quad J' = (J, 1 - y\cdot f) \subseteq R[y]$

$V(J') = \emptyset \Rightarrow 1 = \sum_i a_i f_i + g(1 - y\cdot f)$.

$y \leftarrow 1/f$ and clear denominators $\quad \square$

$\Rightarrow$ " Varieties are in correspondance with radical ideals "

Alg. closure • Let $S \subset k^n$ a set. Then $V(I(S))$ is the smallest

How to compute? variety containing S: $V(I(S)) = \overline{S}$ (Zariski closure).

$\left(S \subseteq V \subseteq V(I(S)) \Rightarrow I(V(I)) \subseteq I(V) \subseteq I(S) \Rightarrow V(I(S)) \subseteq \underset{\overset{\|}{V}}{V(I(V))} \subseteq V(I(V(I))) \right)$

Nullstellensatz allows to relate Zariski closure and ideal quotient.

Lemma: $\overline{V(I) - V(J)} \subseteq V(I : J)$

and if k alg closed and I radical, then this is an equality.

Pf. • We need to show that $(I : J) \subseteq I(V(I) - V(J))$.

Pick $f \in I : J$ and $p \in V(I) - V(J)$.

$\exists g \in J$ such that $g(p) \neq 0$. And $f \cdot g \in I$ so $f(p) \cdot g(p) = 0$

hence $f(p) = 0$ (over a field).

exercise / cvo /

• Now, assume k alg closed, $I = \sqrt{I}$. Pick $p \in V(I : J)$

by def: If $f \cdot g \in I$ for all $g \in J$ then $f(p) = 0$

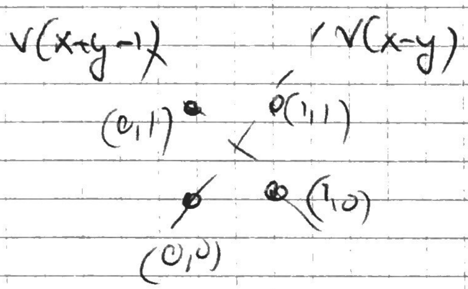
Now let $f \in I(V(I) - V(J))$, then $\underset{g \in J}{f \cdot g}$ vanish on $V(I) \Rightarrow f \cdot g \in \sqrt{I} = I$

so $f \cdot g \in I$ for all $g \in J$ hence $f(p) = 0$ $\Rightarrow f \in I(V(I : J))$ $\square$

Example: $S=\{p_1,\dots,p_4\}=\{(0,0),(0,1),(1,0),(1,1)\}\subseteq \mathbb{A}^2_k$.

$$I(S)=\bigcap_{i=1}^{4} I(p_i)=\left(x^2-x,\ y^2-y\right)$$

Remove the points lying on $x-y$



$$(x^2-x,\ y^2-y):(x-y) = \left(x+y-1,\ y^2-y\right).$$

C2 - Graded Objects and Projective Geometry.

- We used alg. closed field to ensure that $f(x)$ has always $\deg f$ roots.
- Analogously, projective spaces are the right place to count intersections: two lines in $\mathbb{A}^2_k$ can be $\neq$ and $//$ whereas they always intersect in $\mathbb{P}^2_k$ $(k \equiv \mathbb{C})$.

1) Projective Space / Projective varieties

- $\mathbb{A}^n_k$ can be interpreted as k^n

$$\mathbb{P}^n_k := \mathbb{A}^{n+1}_k \Big/ (a_0,\dots,a_n) \sim (b_0,\dots,b_n) \iff \exists \lambda \in k^* : (a_i) = \lambda (b_i)$$

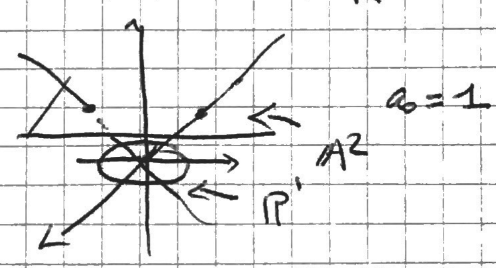
points on the same line through the origin are identified.

homogeneous coord. : $(a_0 : a_1 : \dots : a_n)$ defined up to mult by a nonzero constant.

Hyperplane at ∞: $a_0 = 0$ it is a $\mathbb{P}^{n-1}_k$

Affine part of $\mathbb{P}^n_k$: $a_0 \neq 0$, so points of the form $(1 : \frac{a_1}{a_0} : \dots : \frac{a_n}{a_0})$ it is a $\mathbb{A}^n_k$.

$$\mathbb{P}^n_k = \mathbb{A}^n_k \cup \mathbb{P}^{n-1}_k$$



- To define a variety in proj. space, we need polynomials that vanish on lines through the origine:

$$p \in \mathbb{A}^{n+1}_k : \quad f(p) = 0 \Rightarrow f(\lambda \cdot p) = 0 \quad \forall \lambda \in k^*.$$

- A polynomial is homogeneous if ~~a~~ it is ~~polynomial f~~ such that all ~~its~~ monomials ~~appearing in f~~ are of the same total degree.

A homogeneous pol. defines a variety in $\mathbb{P}^n_k$ (but also $\mathbb{A}^{n+1}_k$.)
Here is a motivation to the use of proj. variety.

THM (Bézout): k alg. closed field
f, g homog. polynomials in $k[x, y, t]$ of degree d, e with no common factor.
Then, the curves $V(f)$ and $V(g)$ in $\mathbb{P}^2_k$ meet in $d \cdot e$ points, counted with multiplicity.

Rk: Two lines in $\mathbb{A}^2$ may not intersect, but they always intersect in $\mathbb{P}^2$.

Def: • A homogeneous ideal is an ideal generated by homogeneous elements.
• A variety in projective space, called proj. variety, is the variety defined by a homog. ideal
• The Zariski topology on $\mathbb{P}^n_k$ is defined by making the proj. varieties closed sets.

2) Graded rings and modules, Hilbert function and series.

- The algebraic counterpart of projective varieties are graded rings and modules.

- A $\mathbb{Z}$-graded ring R is a ring which can be decomposed into homogeneous pieces

$$R = \bigoplus_{i \in \mathbb{Z}} R_i \quad (\text{abelian group})$$

such that if $r_i \in R_i$ and $r_j \in R_j$ then $r_i \cdot r_j \in R_{i+j}$.

A module M over R is graded if $M = \bigoplus M_i$ and if $R_i \cdot M_j \subset M_{i+j}$.

Elements in R_i, M_i, are called homog. element of degree i

Ex: - $R = k[x_1, \ldots, x_n]$ is graded by $\deg(x_i) = 1$.
$R_0 = k$, $R_1 = \langle x_1, \ldots, x_n \rangle_k$, ...

- Quotient of R by a homog. ideal is graded.

$$R/I = \bigoplus_{k \in \mathbb{Z}} R_k / I_k$$

$\llcorner$

- Now, let us assume that k is a field from now on. $R = k[x_1, \ldots, x_n]$. The graded piece R_i are k-vector space, so they have a dimension (as vect. spa).

Ex:
- $\dim_k (k[x]_i) = 1$ for all i
- $\dim_k (k[x,y]_i) = i+1$ for all i
- $\dim_k (k[x_0, -, x_n]_i) = \binom{n+i}{i}$ for all i.

(polynomial in i)

Def: The Hilbert function of a finitely generated graded module M is
$$HF(M,i) := \dim_k (M_i).$$

(**Rk:** M_i is indeed a $R_0 = k$-mod and the finitness is a consequence of M fin. gen.).

Ex: $HF(R,i) = \binom{i+2}{2} = \frac{(i+2)(i+1)}{2}$ $R = k[x,y,z]$

dim. of the vector space of forms of degree i in $\mathbb{P}^2$.

(Conics in $\mathbb{P}^2$ form a $\mathbb{P}^5$).

Notation: Shift in grading. R a graded ring, $k \in \mathbb{N}$

$R(k)$ is the graded ring such that $R(k)_i = R_{k+i}$ $\forall i$

Ex:

deg i	0	1	2	3	...
$HF(k[x,y],i)$	1	2	3	4	...
$HF(k[x,y](-2),i)$	0	0	1	2	3 ...

Ex: $R = k[x,y,z]$ $\quad I = (x^3+y^3+z^3)$

$$\dim \left(R/I\right)_i = \dim R_i/I_i = \dim R_i - \dim I_i$$

I is generated by a single equation in degree 3

so $\dim(I_i) = \dim(R_{i-3}) = \dim\left(R(-3)_i\right)$

$HF(R/I, i)$ =	1	3	6	9	12	15	18	...
i =	0	1	2	3	4	5	6	...

We have $\cancel{H}HF(R/I, i) = \dim(R_i) - \dim(R_{i-3})$

$$= \binom{i+2}{2} - \binom{i-1}{2} = 3i \quad \text{if } i \geq 1.$$

(a <u>polynomial in i</u>).

Now, add a linear form, say x: $J = I + (x)$
(intersection between $x^3+y^3+z^3=0$ and $x=0$).

$R/J \cong k[y,z]/(y^3+z^3)$ and the Hilbert function is

i:	0	1	2	3	4	...
$HF(R/J, i)$:	1	2	3	3	3	...

3 = # intersection pts by Bezout!

Hilbert function can be encoded as follows

Def: The Hilbert series of a finitely generated, graded module M is
$$HS(M,t) = \sum_{i\in\mathbb{Z}} HF(M,i)\, t^i$$

We will see that over $R=k[x_1,\dots,x_n]$, $HS(M,t) = \frac{P(t)}{(1-t)^n}$

where $P(t) \in \mathbb{Z}[t,t^{-1}]$

$\rightsquigarrow$ Macaulay2 examples.

Exercise: It is easy to see that $HS(k[x],t) = 1+t+t^2+\dots = \frac{1}{1-t}$

Show that $HS(k[x_1,\dots,x_n],t) = \frac{1}{(1-t)^n}$. (Induction)

• Artinian rings: a ring is Artinian if there is no infinite proper descending chains of ideals (submodules).

Suppose we have a graded ring such that $R_i \neq 0 \ \forall i \gg 0$.
Then
$$(R_1) \supsetneq (R_2) \supsetneq \cdots \quad \text{infinite desc. chain.}$$

$\rightsquigarrow$ If R is a polynomial ring, M a finitely gen., graded R-mod

M artinian $\iff$ $M_i = 0$ for $i \gg 0$.

Such a module is Artinian $\iff$ $HS(M,t) \in \mathbb{N}[t,t^{-1}]$ (see M2).

3) Hilbert polynomial.

We have observed that the Hilbert function of a pol ring is a polynomial for $i \gg 0$ (and also in an example). This is a general fact that we develop hereafter.

- Graded maps.

A morphism of graded mod $\phi : M \to N$ is graded if

$$\phi(M_i) \subseteq N_i \qquad \forall i.$$

Motivation: taking graded slices of maps, which reduced us to linear algebra.

- A sequence of vector spaces and linear maps

$$V_\bullet : \quad \cdots \to V_{j+1} \xrightarrow{\phi_{j+1}} V_j \xrightarrow{\phi_j} V_{j-1} \to \cdots$$

is a complex if $\mathrm{Im}(\phi_{j+1}) \subseteq \mathrm{Kernel}(\phi_j) \quad \forall j$.

It is exact at position j if $\mathrm{Im}(\phi_{j+1}) = \ker(\phi_j)$.
It is called an exact seq if it is exact everywhere.

The homology of V is defined by $H_j(V_\bullet) := \dfrac{\ker(\phi_j)}{\mathrm{Im}(\phi_{j+1})}$

Exercise (Euler characteristic):

Given a complex $0 \to V_n \to \cdots \to V_0 \to 0$ of finite dim. vector spaces, one has $\chi(V) := \sum_{i=0}^{n} (-1)^i \dim(V_i) = \sum_{i=0}^{n} (-1)^i \dim H_i(V_\bullet)$.

[In particular: V exact $\Rightarrow \chi(V) = 0$.

The above definitions generalize to sequences of modules and graded modules (with graded maps).

Example: R graded ring. $f \in R_i$

The map $R \xrightarrow{\cdot f} R$ is not graded

But $R(-i) \xrightarrow{\cdot f} R$ is graded.

THM: If M is a finitely generated, graded module, then there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that

$$HF(M,i) = f(i) \quad \text{for } i \gg 0.$$

$f(i)$ is called the Hilbert polynomial of M, denoted $HP(M,i)$.

Proof (sketch of): Induct on the number of variables in the ring over M is defined.

- No variable: $R = R_0 = k$, M is a vector space, $HP(M,i) = 0$ $i \gg 0$.

- Suppose it is true for $n-1$ var. We build the exact seq:

$$0 \to K \to M(-1) \xrightarrow{x_n} M \to C \to 0$$

K and C are finitely generated and since x_n kills them they are actually finitely generated other a poly. ring in $n-1$ var.

Thus $HF(M,i) - HF(M,i-1) \in \mathbb{Q}[i]$, $i \gg 0$.

Now, it is a general property:

- Given a function $P: \mathbb{N} \to \mathbb{Z}$ such that $\Delta P(i) := P(i) - P(i-1)$ is a polynomial with rational coeff (for $i \gg 0$), P is itself a polynomial with rat. coeff and has degree one greater than ΔP (exercise; CLO). $\square$

Exercise (Hilbert polynomial of a set of points).

1. For a single point $p \in \mathbb{P}^n_k$, compute $HP(R/_{I(p)}, i)$

$$R/_{I(p)} \simeq \frac{k[x_0, \dots, x_n]}{(x_0, \dots, x_{n-1})} \simeq k[x_n] \qquad HP(R/_{I(p)}, i) = 1$$

2. Let p_1, p_2 two distinct points; prove the exactness of

$$0 \to I(p_1) \cap I(p_2) \to I(p_1) \oplus I(p_2) \to I(p_1) + I(p_2) \to 0$$
$$(f, g) \mapsto f - g$$
$$h \mapsto (h, h)$$

3. $I(p_1) + I(p_2)$ is the defining ideal of $p_1 \cap p_2 = \emptyset$

$$\underbrace{HP(R/_{I(p_1)+I(p_2)}, i)}_{=0} = \cancel{HP(R/_{I(p_1)}, i) + HP(R/_{I(p_2)}, i) - HP(R/_{I})}$$

By induction $HP(R/_{(\cap I(p_i))}, i) = d$.

- Hilbert polynomial contains useful information about the proj. variety $V(I)$.

We will see later that $HP(R/_I, i)$ is of the form

$$\frac{a_m}{m!} i^m + \frac{a_{m-1}}{(m-1)!} i^{m-1} + \dots \qquad a_i \in \mathbb{Z}, \; a_m > 0$$

Def: For a homogeneous ideal $I \subseteq k[x_0, \dots, x_n]$

with $HP(R/_I, i) = \frac{a_m}{m!} i^m + \dots$

we define: - dimension of $V(I) \subseteq \mathbb{P}^n_k$ as m
- codim of ——— as $n-m$
- degree of $V(I) \subseteq \mathbb{P}^n_k$ as a_m.

The idea of dimension and degree is obtained by slicing with hyperplanes. We will prove this in the next lecture.

$\rightsquigarrow$ Examples in M2.