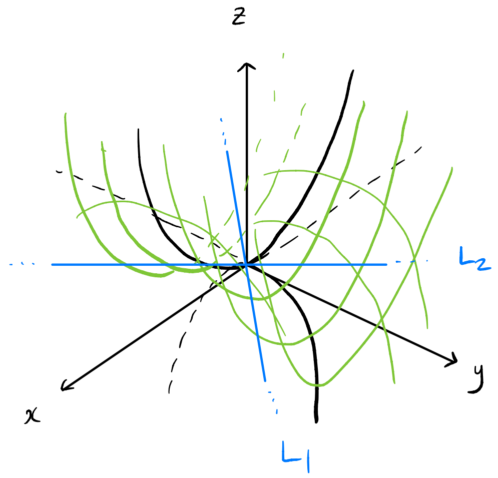
MAG Lecture 5 : Dickson's Lemma

To understand the relationships among affine varieties $V, W \subseteq \mathbb{A}^n$ we need to understand the relation between their ideals $\mathbb{I}(V), \mathbb{I}(W) \subseteq k[x_1, \dots, x_n]$. Suppose we have $\mathbb{I}(V) = \langle f_1, \dots, f_r \rangle$ and $\mathbb{I}(W) = \langle g_1, \dots, g_s \rangle$. Then

CLO Prop 1.4.8

$$
\begin{aligned}
V \subseteq W \quad &\Longleftrightarrow \quad \mathbb{I}(W) \subseteq \mathbb{I}(V) \\
&\Longleftrightarrow \quad g_j \in \mathbb{I}(V) \qquad 1 \le j \le s \\
\text{algebraic} \to \quad &\Longleftrightarrow \quad g_j \text{ can be written as } \textstyle\sum_{i=1}^{r} a_{ji} f_i \text{ for some } a_{ji} \\
\text{geometric} \to \quad &\Longleftrightarrow \quad g_j \text{ vanishes on } V \text{ for all } 1 \le j \le s
\end{aligned}
$$

<u>Example</u> Let $L_1, L_2 \subseteq \mathbb{R}^3$ be the lines $L_1 = \mathbb{V}(z, y-x)$, $L_2 = \mathbb{V}(z, y+x)$. Then with $f = z - (x^2 - y^2)$ the "saddle" we have $L_1 \cup L_2 \subseteq \mathbb{V}(f)$ since $L_1 \subseteq \mathbb{V}(f)$, $L_2 \subseteq \mathbb{V}(f)$ separately. This follows since f vanishes on both. This means



why?

$$\mathbb{I}(\mathbb{V}(f)) \subseteq \mathbb{I}(L_i) = \langle z, y + (-1)^i x \rangle$$

why? $\to$ $\mathbb{I}(\mathbb{V}(f)) = \langle f \rangle$

But this is clear: $f = 1.z - (y + (-1)^{i+1})(y + (-1)^i x)$.

We have two <u>different</u> ways of checking $V \subseteq W$, one more algebraic and one more geometric. Which is easier depends on the problem.

We see from this that the <u>ideal membership problem</u> (e.g. $g_j \in \mathbb{I}(V)$) is fundamental in algebraic geometry: if we have some effective way of answering it, we can use this to effectively answer any question of the form $V \subseteq W$?

To solve this problem we begin with a special class of ideals: the <u>monomial ideals</u>.

Def^n An ideal $I \subseteq k[x_1,\dots,x_n]$ is a monomial ideal if there exists a set $\{x^\alpha\}_{\alpha\in A}$ of monomials (possibly empty and possibly infinite) such that $I = \langle \{x^\alpha\}_{\alpha \in A}\rangle$ is the smallest ideal containing $\{x^\alpha\}_{\alpha\in A}$. Equivalently

$$I = \left\{ \sum_{\alpha\in A} b_\alpha x^\alpha \;\middle|\; b_\alpha \in k[x_1,\dots,x_n] \text{ and only finitely many nonzero} \right\}$$

Lemma Let $I = \langle \{x^\alpha\}_{\alpha\in A}\rangle$ be a monomial ideal. Then

(i) $x^\beta \in I$ iff. $x^\alpha \mid x^\beta$ for some $\alpha \in A$.
(ii) $x^\beta \in I$ iff. $x^\gamma \mid x^\beta$ for some $x^\gamma \in I$
(iii) $f \in I$ iff. every term of f is in I.

ideal membership problem is easy!

Proof (i) One direction is clear. For the other direction, suppose $x^\beta \in I$. Then for some $b_\alpha \in k[x_1,\dots,x_n]$

$$\begin{aligned} x^\beta &= \sum_{\alpha\in A} b_\alpha x^\alpha \\ &= \sum_{\alpha \in A}\Big(\sum_\gamma c_{\gamma\alpha} x^\gamma\Big) x^\alpha \\ &= \sum_{\alpha\in A,\gamma} c_{\gamma\alpha} x^\gamma x^\alpha \end{aligned}$$

$c_{\gamma\alpha} \in k$

This shows every monomial with a nonzero coefficient in x^β (=RHS) is divisible by x^α, some $\alpha \in A$.

(iii) If $f \in I$ then writing $f = \sum a_\beta x^\beta$ for $a_\beta \in k$ and comparing to $f = \sum_{\alpha\in A} b_\alpha x^\alpha$ for $b_\alpha \in k[x_1,\dots,x_n]$ as above we find all x^β with $a_\beta \neq 0$ are divisible by some x^α, $\alpha \in A$. $\square$

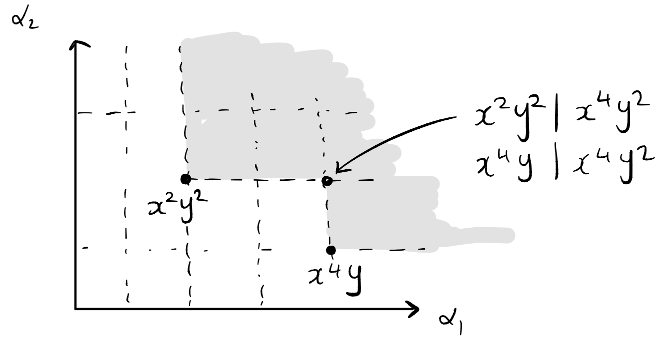
Corollary Two monomial ideals are the same if and only if they contain the same monomials.

Theorem CLO 2.4.5 (Dickson's Lemma) Let $I = \langle \{x^\alpha\}_{\alpha \in A} \rangle$ be a monomial ideal in $k[x_1, \ldots, x_n]$. Then there is a finite subset $A_0 \subseteq A$ with $I = \langle \{x^\alpha\}_{\alpha \in A_0} \rangle$.

Proof The proof is by induction on n. In the base case $n=1$, the set $A \subseteq \mathbb{Z}_{\geqslant 0}$ has a least element μ and clearly $I = \langle \{x^\alpha\}_{\alpha \in A} \rangle = \langle x^\mu \rangle$.

Suppose the claim holds for n variables and let I be a monomial ideal in $k[x_1, \ldots, x_n, y]$ generated by $\{u^\alpha\}_{\alpha \in A}$ (noting $u^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} y^{\alpha_{n+1}}$). If $A \subseteq \mathbb{Z}_{\geqslant 0}^{n+1}$ contained a least element, in the sense that for some $\mu \in A$ we had $u^\mu \mid u^\alpha$ for all $\alpha \in A$ then again $I = \langle u^\mu \rangle$ and we are done. But of course the relation $\mu \leq \alpha$ iff. $u^\mu \mid u^\alpha$ is not a total order, and we need not have such a least element

Example Consider $\langle x^2y^2, x^4y \rangle \subseteq k[x,y]$ where the monomials in the ideal are the "filled in" vertices below

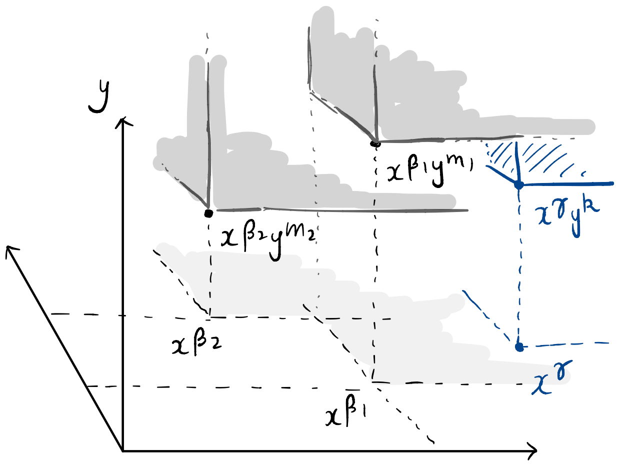


(3.1)

So let us try minimal elements instead, like x^2y^2, x^4y in our picture.

A monomial u^α, $\alpha \in A$ is minimal if there is no $\beta \in A$ distinct from α with $u^\beta \mid u^\alpha$ (i.e. $\beta_i \leq \alpha_i$ for all i). We claim the set $\min(A)$ is finite. Since any u^α, $\alpha \in A$ is divisible by a minimal u^β, this will show $I = \langle \{u^\alpha\}_{\alpha \in A} \rangle = \langle \{u^\beta\}_{\beta \in \min(A)} \rangle$ is finitely generated and complete the inductive step.

To see $\min(A)$ is finite, we compare A to its projection onto the "x-plane". That is, let $B \subseteq \mathbb{Z}^n_{\geqslant 0}$ be the set of all β such that $x^\beta y^m \in I$ for some $m \geqslant 0$.



(4.1)

Set $J = \langle \{x^\beta\}_{\beta \in B} \rangle \subseteq k[x_1, \dots, x_n]$. Let $\min(B)$ denote the set of minimal elements of B. If we take a monomial $u^\alpha = x^\beta y^m$ with $\alpha \in A$ it may not be that β is minimal (see (3.1)). However if $\beta \in B$ <u>is</u> minimal then there is a unique $m \geqslant 0$ such that $\alpha = (\beta, m)$ is in $\min(A)$. To see this, note there is by hypothesis $\alpha = (\beta', m) \in A$ with $\beta \geqslant \beta'$ and by minimality $\beta = \beta'$. If $(\beta, m), (\beta, m')$ are both in A then one is smaller under $\leqslant$, and there is a least pair, proving the claim.

We have thus an injective map $\min(B) \longrightarrow \min(A)$ sending β to this (β, m). By the inductive hypothesis J can be generated by finitely many $B_0 \subseteq B$, and since $\min(B) \subseteq B_0$ this means $\min(B)$ is finite.

Let $x^\gamma y^k$ be such that $(\gamma, k) \in \min(A)$. Then $\gamma \geqslant \beta$ for some $\beta \in \min(B)$. Suppose $(\beta, m) \in \min(A)$. Then by minimality since $\gamma \geqslant \beta$ we must have $k < m$. Thus $x^\gamma y^k$ is "in the shadow" of one of the gray cubes in (4.1). But there are only finitely many of these! Suppose

$$\min(B) = \{\beta_1, \dots, \beta_r\} \quad \text{and} \quad (\beta_1, m_1), (\beta_2, m_2), \dots, (\beta_r, m_r) \in \min(A).$$

Let $M = \max\{m_i \mid 1 \leq i \leq r\}$. Then if $(\gamma, k) \in \min(A)$ we have $k < M$.

In any given y-slice we can only have finitely many elements of $\min(A)$: for any $k < M$ let $B_k = \{\beta \in \mathbb{Z}^n_{\geqslant 0} \mid x^\beta y^k \in I\}$, and $J_k = \langle \{x^\beta\}_{\beta \in B_k} \rangle$. Then again by the inductive hypothesis $\min(B_k)$ is finite and if $\beta \in \min(B_k)$ there is a unique m s.t. $(\beta, m) \in \min(A)$ (note m may be $< k$), so we have maps

$$\begin{tikzcd}
\min(B) \arrow[rr] & & \min(A) \\
& \min(B_0) \arrow[ur] \quad \cdots & \\
& & \min(B_{M-1}) \arrow[u]
\end{tikzcd}$$

The domains of all these maps are finite and we claim they are jointly surjective: if $(\gamma, k) \in \min(A)$ then let $\beta \leq \gamma$ be in $\min(B_k)$. If $\beta \neq \gamma$ then $x^\beta y^k \in I$ contradicts minimality of (γ, k), so $\gamma \in \min(B_k)$ hence (γ, k) is in the image of $\min(B_k) \longrightarrow \min(A)$. From this we conclude $\min(A)$ is finite as claimed. $\square$

<u>Corollary</u> Let $>$ be a relation on $\mathbb{Z}^n_{\geqslant 0}$ satisfying

(i) $>$ is a total order

(ii) if $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geqslant 0}$ then $\alpha + \gamma > \beta + \gamma$.

Then $>$ is a well-ordering if and only if $\alpha \geqslant 0$ for all $\alpha \in \mathbb{Z}^n_{\geqslant 0}$.