Proposition 9.48

Let $I, J_1, \dots, J_r \subset k[x_1, \dots, x_n]$ ideals. Then

$$I : (J_1 + \dots + J_r) = I : J_1 \cap \dots \cap I : J_r \quad \text{and}$$
$$I : (J_1 + \dots + J_r)^\infty = I : J_1^\infty \cap \dots \cap I : J_r^\infty$$

Proof

The general case follows by induction from the $r=2$ case.
By definition

$$I : (J_1 + J_2) = \{ p : \ \forall q \in J_1 + J_2 \ \ pq \in I \}.$$

Since $q \in J_1 + J_2 \Leftrightarrow q = q_1 + q_2,\ q_1 \in J_1\ q_2 \in J_2$, we get

$$pq \in I \ \forall q \in J_1 + J_2 \Leftrightarrow pq_1 + pq_2 \in I \quad \forall q_1 \in J_1\ \forall q_2 \in J_2$$
$$\Leftrightarrow pq_1 \in I \text{ and } pq_2 \in I \ \ \forall q_1 \in J\ \forall q_2 \in J_2$$

("$\Rightarrow$" by considering $(q_1, q_2) = (q_1, 0)$ and $(q_1, q_2) = (0, q_2)$
"$\Leftarrow$" since ideals contain sums)

This proves the first identity. For the second, observe that

$$I : (J_1 + J_2)^\infty = \{ p : \ \forall q \in J_1 + J_2 \ \ \exists N \in \mathbb{N} \ \ pq^N \in I \}$$

and by the binomial formula

$$p(q_1 + q_2)^{N_1 + N_2 - 1} = \sum_{i=0}^{N_1 + N_2 - 1} \binom{N_1 + N_2 - 1}{i} p\, q_1^{N_1 + N_2 - 1 - i} q_2^{\,i}$$
$$= pq_1^{N_1} h_1 + pq_2^{N_2} h_2$$

For some $h_1, h_2 \in k[x_1, \dots, x_n]$. Repeating "$\Rightarrow$" and "$\Leftarrow$" above,

$$\forall q = q_1 + q_2 \in J_1 + J_2 \ \ \exists N \in \mathbb{N} \quad p(q_1 + q_2)^N \in I$$
$$\Leftrightarrow \begin{cases} \forall q_1 \in J_1 \ \ \exists N_1 \in \mathbb{N} \ \ pq_1^{N_1} \in I \\ \forall q_2 \in J_2 \ \ \exists N_2 \in \mathbb{N} \ \ pq_2^{N_2} \in I \end{cases}$$

$\square$

Theorem 9.4.9

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and $q \in k[x_1, \ldots, x_n]$.

(i) If $p_1, \ldots, p_s$ is a basis of $I \cap \langle q \rangle$, then $\frac{p_1}{q}, \ldots, \frac{p_s}{q}$ is a basis of $I : \langle q \rangle$.

(ii) If $f_1, \ldots, f_s$ is a basis of I, and
$$\tilde{I} = \langle f_1, \ldots, f_s, 1 - yq \rangle \subset k[x_1, \ldots, x_n, y]$$
then $I : \langle q \rangle^\infty = \tilde{I} \cap k[x_1, \ldots, x_n]$

Proof

(i) Note that $p \in \langle q \rangle$ implies $p = hq$ for some $h \in k[x_1, \ldots, x_n]$.
Denote $h_i := p_i / q \in k[x_1, \ldots, x_n]$, $i = 1, \ldots, s$.
Then $h_i q = p_i \in I$ so $h_i \in I : \langle q \rangle$.
Let $f \in I : \langle q \rangle$, so $fq \in I$ can be written as
$$fq = \sum_i g_i p_i = \sum_i g_i h_i q \Rightarrow f = \sum_i g_i h_i$$
showing that $h_1, \ldots, h_s$ is a basis of $I : \langle q \rangle$.

(ii) "$\subset$" Let $f \in I : \langle q \rangle^\infty$, so $\exists N \in \mathbb{N}$ $fq^N \in I$. Then
$$fq^N = \sum_i g_i f_i \in \tilde{I} \Rightarrow f = \underbrace{y^N f q^N}_{\in \tilde{I}} + \underbrace{(1 - y^N q^N) f}_{\in \tilde{I}} \in \tilde{I}$$

"$\supset$" Let $f \in \tilde{I} \cap k[x_1, \ldots, x_n]$, so
$$f = f(x) = g_1(x, y) f_1(x) + \cdots + g_s(x, y) f_s(x) + g(x, y)(1 - yq)$$
Evaluating at $y = \frac{1}{q}$ and clearing denominators, we get
$$f q^N = \hat{g}_1(x) f_1(x) + \cdots + \hat{g}_s(x) f_s(x) \in I$$
so $f \in I : \langle q \rangle^\infty$. $\square$

We now have all the ingredients for a method to compute bases for $I:J$ and $I:J^\infty$.

Algorithm 9.50 (Ideal quotient basis)

Given ideals $I=\langle p_1,\dots,p_s\rangle$ and $J=\langle q_1,\dots,q_t\rangle$

1. For each $\ell=1,\dots,t$ compute a basis B_ℓ for $I\cap\langle q_\ell\rangle$ (Theorem 9.29)
2. Compute the bases $\tilde{B}_\ell=\{h/q_\ell : h\in B_\ell\}$ for $I:\langle q_\ell\rangle$ (polynomial division)
3. Compute a basis for $I:J=I:\langle q_1\rangle\cap\dots\cap I:\langle q_t\rangle$ (Theorem 9.33)

   recall $J=\langle q_1\rangle+\dots+\langle q_t\rangle$

Algorithm 9.51 (Saturation basis)

Given ideals $I=\langle p_1,\dots,p_s\rangle$ and $J=\langle q_1,\dots,q_t\rangle$

1. For each $\ell=1,\dots,t$ compute a basis for $I:\langle q_\ell\rangle^\infty=\langle p_1,\dots,p_s,1-yq_\ell\rangle\cap k[x_1,\dots,x_n]$ (Elimination Theorem 8.2)
2. Compute a basis for $I:J^\infty=I:\langle q_1\rangle^\infty\cap\dots\cap I:\langle q_t\rangle^\infty$ (Theorem 9.33)

IRREDUCIBLE VARIETIES

Definition 9.52

A variety $V \subset k^n$ is <u>irreducible</u> if it cannot be written as a finite union of smaller varieties.
That is, if $V = W_1 \cup W_2$ with W_1, W_2 varieties then either $V = W_1$ or $V = W_2$

Example 9.53

(1) $V(xz, yz) = V(x,y) \cup V(z)$ is not irreducible.
(2) $V(y - x^2, z - x^3)$ is irreducible, but how to prove that?

Recall that $V(I) \cup V(J) = V(IJ)$ by Theorem 9.22.
$\rightsquigarrow$ irreducible varieties related to "non-product" ideals.

Definition 9.54

An ideal $I \subset k[x_1, \ldots, x_n]$ is <u>prime</u> if
$$pq \in I \Rightarrow p \in I \text{ or } q \in I$$

Proposition 9.55

Let $V \subset k^n$ be a variety. Then

$$V \text{ irreducible} \iff I(V) \text{ prime}$$

Proof

"$\Rightarrow$" Let $pq \in I(V)$. Set $W_1 = V \cap V(p)$, $W_2 = V \cap V(q)$.

Since pq vanishes everywhere on V, irreducibility gives

$$V = W_1 \cup W_2 \implies V = W_1 \text{ or } V = W_2.$$

If $V = W_1$, then $p \in I(V)$ and if $V = W_2$ then $q \in I(V)$.

"$\Leftarrow$" Suppose $V = W_1 \cup W_2$ for some varieties W_1, W_2.

Suppose $V \neq W_1$. We need to show $V = W_2$

Since $V(I(W)) = W$ for all varieties W, we have

$$V = W_2 \Leftarrow V \subset W_2 \Leftarrow I(V) \supset I(W_2)$$

Let $q \in I(W_2)$. By assumption $W_1 \subsetneq V$, so $I(W_1) \supsetneq I(V)$

i.e. there exists $p \in I(W_1) \setminus I(V)$.

Then pq vanishes on $W_1 \cup W_2 = V$, so $pq \in I(V)$.

$I(V)$ prime and $p \notin I(V) \implies q \in I(V)$

proving that $I(W_2) \subset I(V)$ $\square$

Corollary 9.56

When K is algebraically closed, we have the bijective correspondence

$$\{\text{irreducible varieties}\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{prime ideals}\}$$

Proof

By the ideal-variety correspondence (Theorem 9.9) and Proposition 9.55, it suffices to check that prime ideals are radical. This is immediate, since

$$p^m \in I \Rightarrow p \in I \text{ or } p^{m-1} \in I \quad \text{for } I \text{ prime.} \quad \square$$

Example 9.53(2) revisited

Consider $V = V(y - x^2, z - x^3) \subset \mathbb{R}^3$

Let $pq \in I(V)$. Then $p(t, t^2, t^3) q(t, t^2, t^3) = 0 \ \forall t \in \mathbb{R}$

so either $p(t, t^2, t^3) = 0 \ \forall t \in \mathbb{R}$ or $q(t, t^2, t^3) = 0 \ \forall t \in \mathbb{R}$

$\Rightarrow p \in I(V)$ or $q \in I(V)$

Hence $I(V)$ is prime and V irreducible.

Proposition 9.57

Let $P=(p_1, \dots, p_n): K^m \to K^n$ be a polynomial mapping (that is, each p_i is a polynomial in $K[t_1, \dots, t_m]$)

Let $V = \overline{P(K^m)}$ be the Zariski closure of the image of P.

If K is an infinite field, then V is irreducible.

Proof

By Lemma 9.39(i) $I(V) = I(P(K^m))$.

Let $fg \in I(V)$. Then $f(P(t))g(P(t)) = 0 \ \forall t \in K^m$.

Since K is infinite, this implies that at least one of $f \circ P, g \circ P \in K[t_1, \dots, t_n]$ is the zero polynomial.

So $f \in I(V)$ or $g \in I(V)$ and $I(V)$ is prime. $\square$

Proposition 9.58

Let $R: (\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}): K^m \setminus W \to K^n$ be a rational mapping, where $W = V(q_1 \cdots q_n)$. Let $V = \overline{R(K^m \setminus W)}$.

If K is an infinite field, then V is irreducible.

Proof

If $f \in K[x_1, \dots, x_n]$, then for $t \in K^m \setminus W$

$$f \circ R(t) = 0 \iff (q_1(t) \cdots q_n(t))^N (f \circ R(t)) = 0 \ \forall N \in \mathbb{N}$$

and for large enough N, $(q_1 \cdots q_n)^N (f \circ R) \in K[t_1, \dots, t_m]$.

Since K is infinite and $q_1 \cdots q_n \neq 0$, also $K^m \setminus W$ is infinite.

Repeating the argument of Prop 9.57 shows $I(V)$ is prime $\square$

Definition 9.59

An ideal $I \subset k[x_1, \ldots, x_n]$ is <u>maximal</u> if it is proper (i.e. $I \neq k[x_1, \ldots, x_n]$) and for any ideal J

$$I \subset J \subset k[x_1, \ldots, x_n] \Rightarrow I = J \text{ or } J = k[x_1, \ldots, x_n]$$

Proposition 9.60

Let $a_1, \ldots, a_n \in k$. Then

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subset k[x_1, \ldots, x_n]$$

is maximal.

Proof

Let J be an ideal with $I \subsetneq J$, so $\exists p \in J \setminus I$.
By the division algorithm,

$$p = q_1 \cdot (x_1 - a_1) + \cdots + q_n \cdot (x_n - a_n) + r$$

with $LT(r) < x_i$ for all $i = 1, \ldots, n$, so $r \in k$ is constant.
Since $I \subset J$, it follows that $r = p - \sum q_i (x_i - a_i) \in J$, so $1 \in J$ and $J = k[x_1, \ldots, x_n]$. $\square$

Theorem 9.61

Let k be an algebraically closed field.
Let $I \subset k[x_1, \dots, x_n]$ be a maximal ideal.
Then $\exists a_1, \dots, a_n \in k$ such that $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$.

Proof

By the Weak Nullstellensatz (Theorem 9.2)

$$I \neq k[x_1, \dots, x_n] \Rightarrow V(I) \neq \emptyset$$

Let $a = (a_1, \dots, a_n) \in V(I) \subset k^n$. Then we have

$$I \subset I(V(I)) \subset I(\{a\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle.$$

By maximality $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. $\square$

Corollary 9.62

Let k be an algebraically closed field.
Then we have the bijective correspondence

$$\{\text{points}\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{maximal ideals}\}$$

Proof

By Prop 9.60 and Thm 9.61, maximal ideals are exactly the ideals $\langle x_1 - a_1, \dots, x_n - a_n \rangle = I(\{(a_1, \dots, a_n)\})$ $\square$