Definition 9.14

Let $p, q \in K[x_1, \dots, x_n]$. A polynomial $h \in K[x_1, \dots, x_n]$ is a <u>greatest common divisor</u> of p and q, if

(i) $h \mid p$ and $h \mid q$

(ii) if $f \mid p$ and $f \mid q$, then $f \mid h$

We will denote $h = \gcd(p, q)$.

Note: $\gcd(p, q)$ is only unique up to a constant factor.

Proposition 9.15

Let K be a field of characteristic 0 (i.e. $\mathbb{Q} \subset K$). Then for any $I = \langle p \rangle$, $p \in K[x_1, \dots, x_n]$,

$$p_{red} = \frac{p}{\gcd\left(p, \frac{\partial p}{\partial x_1}, \dots, \frac{\partial p}{\partial x_n}\right)}$$

Proof

Let $p = c \cdot p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ be the decomposition of p into distinct irreducibles $p_i \in K[x_1, \dots, x_n]$, $0 \neq c \in K$, $\alpha_i \geq 1$.

It suffices to show that

$$\gcd\left(p, \frac{\partial p}{\partial x_1}, \dots, \frac{\partial p}{\partial x_n}\right) = p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1} =: h$$

We see that $h \mid p$ and by the Leibniz rule

$$\frac{\partial p}{\partial x_i} = c \cdot h \cdot \left(\alpha_1 \cdot \frac{\partial p_1}{\partial x_i} \cdot p_2 \cdots p_m + \dots + \alpha_m \cdot p_1 \cdots p_{m-1} \frac{\partial p_m}{\partial x_i}\right)$$

so also $h \mid \frac{\partial p}{\partial x_i}$ for all $i = 1, \dots, m$.

It remains to show that h is the greatest. Since any factor $f | p$ must be some product of the irreducibles $p_1 \to p_m$, it suffices to show that $\forall i \; \exists j$ such that $p_i^{\alpha_i} \nmid \frac{\partial p}{\partial x_j}$

Write

$$p = c \cdot p_1^{\alpha_1} \cdots p_m^{\alpha_m} = p_i^{\alpha_i} \cdot q$$

Then we see

$$\frac{\partial p}{\partial x_j} = \alpha_i p_i^{\alpha_i - 1} \cdot \frac{\partial p_i}{\partial x_j} \cdot q + p_i^{\alpha_i} \frac{\partial q}{\partial x_j}$$

$$= p_i^{\alpha_i - 1} \left(\alpha_i \frac{\partial p}{\partial x_j} q + p_i \cdot \frac{\partial q}{\partial x_j} \right)$$

Suppose $p_i^{\alpha_i} \mid \frac{\partial p}{\partial x_j}$, then since p_i is irreducible, we get

$$p_i \mid \frac{\partial p_i}{\partial x_j} \cdot q \quad \Rightarrow \quad p_i \mid \frac{\partial p_i}{\partial x_j} \text{ or } p_i \mid q$$

However q_i is a product of irreducibles p_l, $l \neq i$.

Hence $p_i \mid \frac{\partial p_i}{\partial x_j}$. Since $\deg\left(\frac{\partial p_i}{\partial x_j}\right) < \deg(p_i)$, this is only possible if $\frac{\partial p_i}{\partial x_j} = 0$.

Since p_i is irreducible, it is nonconstant, so $\frac{\partial p_i}{\partial x_j} \neq 0$ for any x_j that appears in p_i.

So we have shown $p_i^{\alpha_i} \nmid \gcd(p, \frac{\partial p}{\partial x_1} - \frac{\partial p}{\partial x_n})$

$$\Rightarrow h = p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1} = \gcd\left(p, \frac{\partial p}{\partial x_1} \to \frac{\partial p}{\partial x_n}\right) \quad \square$$

<u>Remark</u>: in fields of positive characteristic this may fail: If $2 = 0$, then $p = x^2 + y^2 + z^2$ has $\frac{\partial p}{\partial x} = \frac{\partial p}{\partial y} = \frac{\partial p}{\partial z} = 0$.

SUMS OF IDEALS

Definition 9.16

The sum of $I, J \subset k[x_1, \ldots, x_n]$ is
$$I + J := \{p + q : p \in I, q \in J\}$$

Proposition 9.17

If $I, J \subset k[x_1, \ldots, x_n]$ ideals, then $I+J$ is an ideal. Moreover if $I = \langle p_1, \ldots, p_s \rangle$, $J = \langle q_1, \ldots, q_t \rangle$ then
$I + J = \langle p_1, \ldots, p_s, q_1, \ldots, q_t \rangle$ so
$I+J$ is the smallest ideal containing I and J.

Proof

$I+J$ is an ideal:

- $0 \in I$ and $0 \in J \Rightarrow 0 = 0 + 0 \in I + J$
- if $f_1, f_2 \in I+J$ then $f_1 = p_1 + q_1$, $f_2 = p_2 + q_1$
  $\Rightarrow f_1 + f_2 = (p_1 + p_2) + (q_1 + q_2) \in I + J$
- if $f = p + q \in I+J$ and $h \in k[x_1, \ldots, x_n]$ then
  $fh = ph + pq \in I + J$

$I + J = \langle p_1, \ldots, p_s, q_1, \ldots, q_t \rangle$:

"$\supseteq$" $p_1 + 0, \ldots, p_s + 0, 0 + q_1, \ldots, 0 + q_t \in I + J$

"$\subseteq$" Let $p + q \in I + J$. Write $p = \sum f_i p_i$ $q = \sum h_i q_i$
Then $p + q = \sum f_i p_i + \sum h_i q_i \in \langle p_1, \ldots, p_s, q_1, \ldots, q_t \rangle$.

$\square$

Corollary 9.18

If $p_1, \dots, p_s \in k[x_1, \dots, x_n]$, then
$$\langle p_1, \dots, p_s \rangle = \langle p_1 \rangle + \dots + \langle p_s \rangle$$

Theorem 9.19

If $I, J \subset k[x_1, \dots, x_n]$ ideals, then
$$V(I+J) = V(I) \cap V(J) \subset k^n$$

Proof

Let $I = \langle p_1, \dots, p_s \rangle$, $J = \langle q_1, \dots, q_t \rangle$. Then by Proposition 9.17
$$V(I+J) = V(p_1, \dots, p_s, q_1, \dots, q_t)$$
$$= V(p_1, \dots, p_s) \cap V(q_1, \dots, q_t) = V(I) \cap V(J) \quad \square$$

PRODUCTS OF IDEALS

Definition 9.20

The product of $I, J \subset k[x_1, \dots, x_n]$ is
$$IJ := I \cdot J := \operatorname{span}_k \{ pq : p \in I, q \in J \}$$
$$= \left\{ \sum_{i=1}^{m} p_i q_i : p_1, \dots, p_m \in I, q_1, \dots, q_m \in J, m \in \mathbb{N} \right\}$$

Proposition 9.21

If $I, J \subset k[x_1, \ldots, x_n]$ ideals, then $I \cdot J$ is an ideal.

Moreover if $I = \langle p_1, \ldots, p_s \rangle$, $J = \langle q_1, \ldots, q_t \rangle$, then

$$I \cdot J = \langle p_i q_j : 1 \le i \le s, \ 1 \le j \le t \rangle$$

Proof

$I \cdot J$ is an ideal:

- $0 \in I$, $0 \in J \Rightarrow 0 = 0 \cdot 0 \in I \cdot J$
- $f, g \in I \cdot J \Rightarrow f + g \in I \cdot J$
  (since $f+g = 1 \cdot f + 1 \cdot g$ is a k-linear combination)
- $f = \sum p_i q_i \in I \cdot J$, $h \in k[x_1, \ldots, x_n]$
  $\Rightarrow fh = \sum (hp_i) q_i \in I \cdot J$

$I \cdot J = \langle p_i q_j : 1 \le i \le s, \ 1 \le j \le t \rangle$:

"$\supset$" Follows from each $p_i q_j \in I \cdot J$.

"$\subset$" Let $f = pq \in I \cdot J$ for some $p \in I$, $q \in J$.

Then we have

$$p = \sum_{i=1}^{s} h_i p_i, \quad q = \sum_{j=1}^{t} g_j q_j$$

so

$$f = pq = \sum_{i=1}^{s} \sum_{j=1}^{t} (h_i g_j) p_i q_j \subset \langle p_i q_j : \begin{smallmatrix} 1 \le i \le s \\ 1 \le j \le t \end{smallmatrix} \rangle$$

Every element of $I \cdot J$ is a sum of such elements f $\square$

Theorem 9.22

If $I, J \subset k[x_1, \ldots, x_n]$ are ideals, then

$$V(I \cdot J) = V(I) \cup V(J)$$

Proof

"$\subset$" Let $a \in V(I \cdot J)$. Then $p(a)q(a) = 0 \ \forall p \in I, q \in J$.

Either

(i) $p(a) = 0 \ \forall p \in I \implies a \in V(I)$

or

(ii) $\exists p \in I \ p(a) \neq 0 \implies q(a) = 0 \ \forall q \in J \Rightarrow a \in V(J)$

"$\supset$" $I \cdot J \subset I \Rightarrow V(I) \subset V(I \cdot J)$

$I \cdot J \subset J \Rightarrow V(J) \subset V(I \cdot J)$ $\square$

INTERSECTION OF IDEALS

Proposition 9.23

If $I, J \subset K[x_1, \ldots, x_n]$ ideals, then $I \cap J$ is an ideal.

Proof

- $0 \in I$, $0 \in J \Rightarrow 0 \in I \cap J$
- $p, q \in I \cap J \Rightarrow p + q \in I$ and $p + q \in J \Rightarrow p + q \in I \cap J$.
- $p \in I \cap J$, $h \in k[x_1, \ldots, x_n] \Rightarrow ph \in I$ and $ph \in J \Rightarrow ph \in I \cap$

$\square$

Example 9.24

Computing generators of $I \cap J$ is not as easy as for $I+J$ and IJ !

Let

$$I = \langle p \rangle, \quad p = (x+y)^4 (x^2+y)^2 (x-5y)$$
$$J = \langle q \rangle, \quad q = (x+y)(x^2+y)^3(x+3y)$$

Then

$$I \cap J = \langle f \rangle, \quad f = (x+y)^4 (x^2+y)^3 (x-5y)(x+3y)$$

since $h \in I \cap J \iff p \mid h$ and $q \mid h$

Consequence: any computation of generators of $I \cap J$ has to directly or indirectly deal with irreducible factors.

Definition 9.25

Let $p, q \in k[x_1, \ldots, x_n]$. A polynomial $h \in k[x_1, \ldots, x_n]$ is a least common multiple of p and q if

(i) $p \mid h$ and $q \mid h$

(ii) if $p \mid f$ and $q \mid f$ then $h \mid f$.

We will denote $h = \operatorname{lcm}(p, q)$

Note: again $\operatorname{lcm}(p,q)$ is only unique up to a constant.

Example 9.26

Consider the factorizations into distinct irreducibles

$$p = c \cdot f_1^{\alpha_1} \cdots f_m^{\alpha_m} \cdot p_1^{\gamma_1} \cdots p_s^{\gamma_s}$$
$$q = \tilde{c} \cdot f_1^{\beta_1} \cdots f_m^{\beta_m} \cdot q_1^{\delta_1} \cdots q_t^{\delta_t}$$

where

- $c, \tilde{c} \in K$ nonzero
- $f_1, \dots, f_m, p_1, \dots, p_s, q_1, \dots, q_t \in K[x_1, \dots, x_n]$ distinct irreducibles
- $\alpha_i, \beta_i, \gamma_i, \delta_i \geq 1 \quad \forall i$
- $f_i \mid p$ and $f_i \mid q \quad \forall i = 1 \dots m$
- $p_i \mid p$ and $p_i \nmid q \quad \forall i = 1 \dots s$
- $q_i \nmid p$ and $q_i \mid q \quad \forall i = 1, \dots, t$

Then

$$\operatorname{lcm}(p,q) = f_1^{\max(\alpha_1, \beta_1)} \cdots f_m^{\max(\alpha_i, \beta_i)} \cdot p_1^{\gamma_1} \cdots p_s^{\gamma_s} \cdot q_1^{\delta_1} \cdots q_t^{\delta_t}$$

Proposition 9.27

Let $I = \langle p \rangle$ and $J = \langle q \rangle$ principal ideals in $K[x_1, \dots, x_n]$.
Then $I \cap J$ is a principal ideal and
$$I \cap J = \langle \operatorname{lcm}(p,q) \rangle$$

Proof Let $h = \operatorname{lcm}(p,q)$.

"$\supset$" Since $p \mid h$ and $q \mid h$, we get $\langle h \rangle \subset I \cap J$

"$\subset$" If $f \in I \cap J$ then $p \mid f$ and $q \mid f$.
Then $h \mid f$, so $f \in \langle h \rangle$. $\square$

Proposition 9.28

Let $p, q \in K[x_1, \ldots, x_n]$. Then

$$\mathrm{lcm}(p,q) \cdot \gcd(p,q) = pq.$$

(Warning: lcm & gcd only defined up to a constant!
A more formal statement: $\exists h, g$ s.t. h is a lcm
and g is a gcd such that $hg = pq$)

Proof

Write p, q in distinct irreducibles as in Example 9.26.
Then $\gcd(p,q) = f_1^{\min(\alpha_1, \beta_1)} \cdots f_m^{\min(\alpha_m, \beta_m)}$
and the claim follows from

$$\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta$$

since

$$\begin{aligned}
&\mathrm{lcm}(p,q) \cdot \gcd(p,q) \\
&= \left(\prod f_i^{\max(\alpha_i, \beta_i)} \cdot \prod p_i^{\gamma_i} \cdot \prod q_i^{\delta_i}\right)\left(\prod f_i^{\min(\alpha_i, \beta_i)}\right) \\
&= \left(\prod f_i^{\alpha_i} \prod p_i^{\gamma_i}\right)\left(\prod f_i^{\beta_i} \prod q_i^{\delta_i}\right) = \frac{1}{c\tilde{c}} pq
\end{aligned}$$

$\square$

Consequence: Given p, q, if we can find h such that $\langle p \rangle \cap \langle q \rangle = \langle h \rangle$, then

$$\gcd(p,q) = \frac{pq}{h}$$