Questions:

- Find generators of $\sqrt{I}$
- check if I is radical
- $f \in \sqrt{I}$ — radical membership

Start with $f \in \sqrt{I}$

Note: check if $f^m \in I \quad \forall m > 0$ is not so good...—

Prop 1 (Rad. membership). K - arbitary field

$I = (f_1, \dots, f_s) \subseteq K[x_1, \dots, x_n]$ an ideal.

$f \in \sqrt{I}$ if $1 \in \hat{I} = (f_1, \dots, f_s, 1 - yf) \subseteq K[x_1, \dots, x_n, y]$

i.e. $\hat{I} = K[x_1, \dots, x_n, y]$.

Aside: if $f \in \sqrt{I} \Rightarrow f \in I(V(I))$

$V(I) = V(\text{stuff}) \cap V(f)$

Proof: From Proof Hilbert's Nullstelen Statz we

$1 \in \hat{I} \Rightarrow f^m \in I$ for some $m \Rightarrow f \in \sqrt{I}$

Now Suppse $f \in \sqrt{I} \Rightarrow f^m \in I \subseteq \hat{I}$

but $1 - yf \in \hat{I}$

$$1 = y^m f^m + (1 - y^m f^m)$$

$$= \underbrace{y^m f^m}_{\in \hat{I}} + \underbrace{(1 - yf)}_{\in \hat{I}} \underbrace{(1 + yf + \cdots + y^{m-1} f^{m-1})}_{\in \hat{I}}$$

$\Rightarrow 1 \in \hat{I}$. ∎

Radical Memembership Alg.

IS $f \in \sqrt{(f_1, \ldots, f_s)} \subseteq K[x_1, \ldots, x_n]$

- Compute a reduced GB of $(f_1, \ldots, f_s, 1 - yf)$
- If GB $= \{1\} \Rightarrow f \in \sqrt{I}$
  otherwise $f \notin \sqrt{I}$.

Prop Let $f \in K[x_1, \ldots, x_n]$ $I = (f)$

If $f = c f_1^{a_1} \cdots f_r^{a_r}$ is the (unique upto constant) factorization of f into a prod. of distinct irreducible poly. Then

$c \in K$

$$\sqrt{I} = \sqrt{(f)} = (f_1 \cdots f_r)$$

Proof: Show $f_1 \cdots f_r \in \sqrt{I}$

$N > \max(a_1, \ldots, a_n)$

$\Rightarrow c(f_1 \cdots f_r)^N = f_1^{N-a_1} \cdots f_r^{N-a_n} \cdot f$ ($= c f_1^{a_1} \cdots f_r^{a_r}$)

$\Rightarrow (f_1 \cdots f_r)^N \in I \Rightarrow f_1 \cdots f_r \in \sqrt{I}$

Now suppose $g \neq 0 \in \sqrt{I} \Rightarrow g^m \in I = (f)$

$\Rightarrow g^m = h \cdot c f_1^{a_1} \cdots f_r^{a_r}$, $h \in K[x_1, \ldots, x_n]$

But each f_i is irriducible $\therefore$ If it appears in g^m it must appear in g

Since $g^m = g \cdots g$ $\therefore g = \tilde{h} f_1 \cdots f_r$ ($\tilde{h} \in K[x_1, \ldots, x_n]$)

$\therefore g \in (f_1 \cdots f_r)$. ∎

Def: If $f \in K[x_1, \ldots, x_n]$ is a poly. we define the **reduction** of f, f_{red}, to be s.t.

$$(f_{red}) = \sqrt{(f)}$$

If $f = f_{red}$ (⇔ say) f is **reduced** or **square-free**.

Ex) $f = (x + y^2)^7 (x-y)^{302}$

$$f_{red} = (x+y^2)(x-y)$$

(only unique upto a constant)

Can we compute f_{red} without factoring?

Yes !!

Def: Let $f, g \in K[x_1, \ldots, x_n]$, $h \in K[x_1, \ldots, x_n]$ is called the greatest common divisor of f, g

i.e.

$$h = \gcd(f, g)$$

if:

(i) h divides f and g

(ii) If $p \mid f$, $p \mid g \Rightarrow p \mid h$ ($p \in K[x_1, \ldots, x_n]$)

there is an algorithm to compute $\gcd(f_1, \dots, f_s)$ in 4.3

Prop: Suppose K is a field containg $\mathbb{Q}$. Let $I = (f) \subseteq K[x_1, \dots, x_n]$. Then $\sqrt{I} = (f_{red})$ where

$$f_{red} = \frac{f}{\gcd\left(f, \frac{df}{dx_1}, \dots, \frac{df}{dx_n}\right)}$$