Ex $\varphi: V(XY-1) \longrightarrow K$
$(x,y) \longmapsto x$

has image $K \setminus \{0\}$. $\Rightarrow \varphi$ is dominant

$\varphi^*: K[T] \longrightarrow K[X,Y]/(XY-1) \cong K[X, \frac{1}{X}]$
$T \longmapsto X$

is injective.

Rmk The composition of two dominant morphisms is dominant.

Thm 7.5 $\varphi^*: \Gamma(W) \to \Gamma(V)$ is surjective if and only if $\varphi(V) \subseteq W$ is an algebraic subset and $\varphi: V \to \varphi(V)$ is an isomorphism. (φ is an isom. onto its image)

Pf Let $I = \ker(\varphi^*) \subseteq \Gamma(W)$.

Let $W' = \mathcal{V}_W(I) \subseteq W$. Then, $\varphi(V) \subseteq W'$.

Note that I is a radical ideal of $\Gamma(W)$ because $\Gamma(V)$ is a reduced ring.

$\Rightarrow \Gamma(W') = \Gamma(W)/I$.

~~We have an isomorphism~~ $\cancel{\varphi^*: \underset{\Gamma(W')}{\Gamma(W)/I} \to \Gamma(V)}$,

~~which corresponds to~~ $\cancel{\varphi:}$

The morphism $\varphi: V \to W'$ corr. to the injective ring hom. $\varphi^*: \underset{\Gamma(W')}{\underset{\shortparallel}{\Gamma(W)/I}} \longrightarrow \Gamma(V)$.

$\Rightarrow$ By Thm 7.4, we have $\overline{\varphi(V)} = W'$.

If φ^* is surjective, this map $\varphi: V \to W'$ is an isomorphism (in part. $\varphi(V) = W'$).

If $\varphi(V) \subseteq W$ is an alg. subset ($\Rightarrow W' = \varphi(V)$) and $\varphi: V \to \varphi(V)$ is an isom., then $\varphi^*: \Gamma(W') \to \Gamma(V)$ is an isom., in particular surjective. $\square$

<u>Exe</u> $\varphi : K \longrightarrow K^2$ is an isomorphism onto its image $V(X^2-Y)$

$t \longmapsto (t, t^2)$

with inverse map

$x \longleftarrow (x, y)$.

$\varphi^* : K[X,Y] \longrightarrow K[T]$ is surjective.

$X \longmapsto T$

$Y \longmapsto T^2$

8. Gröbner bases

References:

- Sturmfels: What is a Gröbner basis?
- Cox, Little, O'Shea: Ideals, Varieties, and Algorithms (Chapter 2)

Question

How to determine whether a polynomial h lies in an ideal $I = (f_1, \dots, f_m) \subseteq K[x_1, \dots, x_n]$?

Ex If $n = 1$, we can compute $g := \gcd(f_1, \dots, f_m)$ using the Euclidean algorithm. Then, $I = (f_1, \dots, f_m) = (g)$, so $h \in I \iff g \mid h$.

Ex If the polynomials $f_1, \dots, f_m$ have degree ≤ 1, use Gaussian elimination to put the equations into row echelon form.

Def Let $\mathcal{S} := \mathcal{S}(X_1,\dots,X_n) = \{X_1^{e_1}\cdots X_n^{e_n} \mid e_1,\dots,e_n \geq 0\}$ be the set of monomials in $X_1,\dots,X_n$.

A monomial order is a total order $\leq$ on $\mathcal{S}$ such that:

a) $1 \leq M \quad \forall M \in \mathcal{S}$

b) If $M \leq N$, then $MU \leq NU \quad \forall U \in \mathcal{S}$.

Rmk Some people omit condition a), which ensures that $\leq$ is a well-order: every $\emptyset \neq T \subseteq \mathcal{S}$ has a smallest element.

Ese If $n=1$, there is just one monomial order:

$$1 < X_1 < X_1^2 < X_1^3 < \dots$$

Ese lexicographic order

$$X_1^{a_1}\cdots X_n^{a_n} < X_1^{b_1}\cdots X_n^{b_n}$$

$\iff (a_1,\dots,a_n) < (b_1,\dots,b_n)$ lexicographically

$\iff a_1 = b_1, \dots, a_{i-1} = b_{i-1},\ a_i < b_i$ for some $1 \leq i \leq n$.

$$1 < X_2 < X_2^2 < X_2^3 < \dots < X_1 < X_1X_2 < X_1X_2^2 < \dots < X_1^2 < \dots$$

Ex Degree lexicographic order

...

$\Leftrightarrow (a_1+\dots+a_n, a_1,\dots,a_n) < (b_1+\dots+b_n, b_1,\dots,b_n)$
lexicographically

$1 < X_2 < X_1 < X_2^2 < X_1X_2 < X_1^2 < X_2^3 < \dots$

Ex Degree reverse lexicographic order

...

$\Leftrightarrow (a_1+\dots+a_n, -a_n,\dots,-a_1) < (b_1+\dots+b_n, -b_n,\dots,-b_1)$
lexicographically

Rmk For $n=2$, deg. lex. = deg. rev. lex.

Def Let $f = \sum_{M \in S} c_M M \in K[X_1,\dots,X_n]$.

A monomial M occurs in f if $c_M \neq 0$.

Let $f \neq 0$.

Its leading monomial (w.r.t. $\le$) is

$lm(f) := \max\{M \text{ occuring in } f\}$.

Its leading coefficient (w.r.t. $\le$) is

$lc(f) = c_{lm(f)}$.

Its leading term (w.r.t. $\le$) is

$lt(f) = lc(f) \cdot lm(f)$.

Rmk $\mathrm{lm}(fg) = \mathrm{lm}(f)\cdot \mathrm{lm}(g)$ for any $f, g \neq 0$.
$\quad\;\mathrm{lt} \qquad\qquad \mathrm{lt} \qquad \mathrm{lt}$
$\quad\;\mathrm{lc} \qquad\qquad \mathrm{lc} \qquad \mathrm{lc}$

Def A polynomial $f \in K[X_1, \dots, X_n]$ is reduced w.r.t. a subset $G \subseteq K[X_1, \dots, X_n]$ if no monomial M occuring in f is divisible by the leading monomial of any $0 \neq g \in G$.

Ex X^3 is reduced w.r.t. $\{Y, XY+1\}$.

$X^2Y^3 + X^5$ isn't reduced w.r.t. $\{\underline{X^3}+Y\}$ and deg. lex. ordering. (or any other order!)

Rmk For $f = \sum_M c_M M$, let

$$W(f) = \{M : c_M \neq 0 \text{ and } \mathrm{lm}(g) \mid M \text{ for some } 0 \neq g \in G\}.$$

If $W(f) \neq \emptyset$, let $N^{(1)} = \max(W(f))$, $\mathrm{lm}(g) \mid N^{(1)}$, $0 \neq g \in G$.

Consider $$f^{(1)} := f - \frac{c_{N^{(1)}} N^{(1)}}{\mathrm{lt}(g)} \cdot g.$$

Then $M < N^{(1)} \quad \forall M \in W(f^{(1)})$.

Continue this process

$(f \rightsquigarrow f^{(1)} \rightsquigarrow f^{(2)} \rightsquigarrow \dots)$

$N^{(1)} > N^{(2)} > N^{(3)} > \dots$

Since $\leq$ is a well-order, this process has to terminate with some $f^{(k)}$ which is reduced w.r.t. G.

Def A reduction of f w.r.t. G is a polynomial r, which is reduced w.r.t. G and such that

$$r = f - g_1 h_1 - \dots - g_r h_r$$

for some $g_1, \dots, g_r \in G$, $h_1, \dots, h_r \in k[X_1, \dots, X_n]$ with $lm(g_i h_i) \leq lm(f)$.

Rmk $r \equiv f \bmod \underbrace{(G)}_{\text{ideal generated by } G}$.

Ex Use lex. order on $S(X,Y)$.

$f = XY^2 + 1$, $\quad G = \{XY+1, Y+1\}$

$f^{(1)} = XY^2 + 1 - Y(XY+1) = -Y + 1$

$r = f^{(2)} = -Y + 1 + Y + 1 = 2$

or: $f^{(1)} = XY^2 + 1 - XY(Y+1) = -XY + 1$

$r = f^{(2)} = -XY + 1 + X(Y+1) = X + 1$

$\rightsquigarrow$ Warning: Reductions aren't always unique!