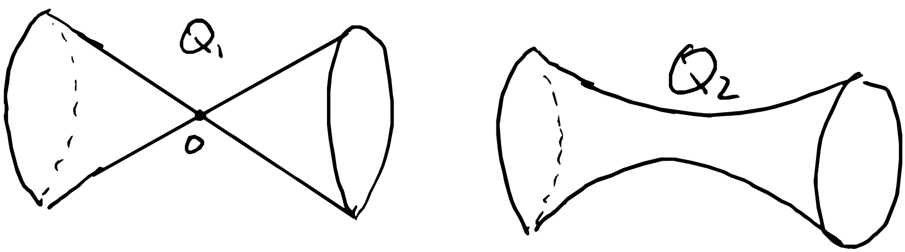
Example 10.11

Consider two surfaces

$$Q_1 = V(q_1) \subset \mathbb{R}^3, \quad q_1 = x^2 - xy - y^2 + z^2$$
$$Q_2 = V(q_2) \subset \mathbb{R}^3, \quad q_2 = x^2 - y^2 + z^2 - z$$



and their intersection curve

$$C = Q_1 \cap Q_2 = V(q_1, q_2) \subset \mathbb{R}^3$$

This intersection is also given by

$$C = V(q_1, q_1 + a q_2), \quad 0 \neq a \in \mathbb{R}$$

so to understand C, we may consider

$$C \subset V(q_1 - q_2) = V(z - xy)$$

$V(z-xy)$ is isomorphic to $\mathbb{R}^2$ by the polynomial mappings

$$\alpha : \mathbb{R}^2 \to V(z-xy) \quad \alpha(x,y) = (x, y, xy)$$
$$\pi : V(z-xy) \to \mathbb{R}^2 \quad \pi(x,y,z) = (x,y)$$

$(\alpha \circ \pi = id_{V(z-xy)}$ and $\pi \circ \alpha = id_{\mathbb{R}^2})$

Hence we may study C through

$$\pi(C) = \pi(V(q_1, q_2)) = V(\alpha^* q_1, \alpha^* q_2)$$
$$= V(x^2y^2 + x^2 - xy - y^2) =: W$$

where the second equality is due to

$$q \circ \alpha = 0 \text{ on } \pi(C) \iff q = q \circ \alpha \circ \pi = 0 \text{ on } C$$

(Indeed if $b \in \pi(C)$ then $b = \pi(a)$ with $a \in C$, so

$$0 = q_i(a) = q_i \circ \alpha \circ \pi(a) = q_i \circ \alpha(b) \implies \pi(C) \subset V(\alpha^* q_1, \alpha^* q_2)$$

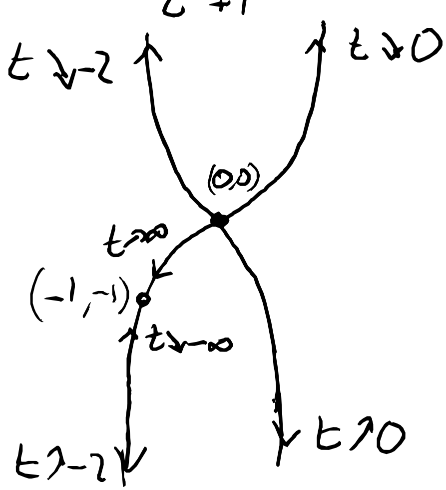
and conversely if $b \in V(\alpha^* q_1, \alpha^* q_2)$ then

$$q_i \circ \alpha(b) = 0 \implies \alpha(b) \in C \text{ and } b = \pi(\alpha(b)) \in \pi(C))$$

Another perspective: on C we have $z = xy$, and $\alpha^* q(x,y) = q \circ \alpha(x,y) = q(x, y, xy)$ is exactly the substitution $z = xy$.

The variety W can be parametrized by

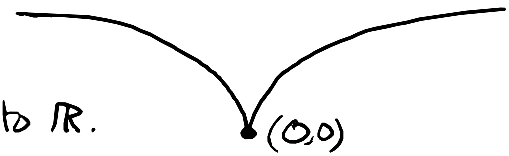
$$x = \frac{-t^2 + t + 1}{t^2 + 1} \qquad y = \frac{-t^2 + t + 1}{t(t+2)}, \qquad t \in \mathbb{R} \setminus \{0, 2\}$$



with $t \to \pm\infty$ giving $(-1,-1) \in W$.

Example 10.12

$V = V(y^5 - x^2) \subset \mathbb{R}^2$



Claim: V is not isomorphic to $\mathbb{R}$.

Proof: suppose there were an isomorphism $\tilde{\alpha} : \mathbb{R} \to V$

Let $c \in \mathbb{R}$ be such that $\tilde{\alpha}(c) = (0,0)$.

Then $\alpha : \mathbb{R} \to V$, $\alpha(t) = \tilde{\alpha}(t-c)$ is also an isomorphism and $\alpha(0) = (0,0)$.

Then the pullback $\alpha^* : K[V] = \mathbb{R}[x,y]/\langle y^5 - x^2 \rangle \to \mathbb{R}[t]$ would be a ring isomorphism with

$$\alpha^*([x]) = p \in K[t]$$
$$\alpha^*([y]) = q \in K[t]$$

so

$$0 = \alpha^*([y^5 - x^2]) = q^5 - p^2 \in K[t]$$

The choice $\alpha(0) = (p(0), q(0)) = (0,0)$ implies

$$p = c_1 t + c_2 t^2 + \dots + c_n t^n$$
$$q = d_1 t + d_2 t^2 + \dots + d_m t^m$$

Comparing coefficients in $q^5 = p^2$, we see that

$$p^2 = c_1^2 t^2 + 2c_1c_2 t^3 + (c_2^2 + 2c_1c_3) t^4 + 2(c_1c_4 + c_2c_3) t^5 + \dots$$
$$q^5 = 0 \cdot t^2 + 0 \cdot t^3 + 0 \cdot t^4 + d_1^5 t^5 + \dots$$

$$\left.\begin{array}{l} t^2 \text{ coefficients} \Rightarrow c_1 = 0 \\ t^4 \text{ coefficients} \Rightarrow c_2 = 0 \\ t^5 \text{ coefficients} \Rightarrow d_1 = 0 \end{array}\right\} \Rightarrow \text{ $\alpha^* K[x,y]$ only contains constants and polynomials of $\deg \geq 2$ } \lightning.$$

Recall Prop 7.8:

Given an ideal $I \subset k[x_1, \ldots, x_n]$ and a Groebner basis $G \subset I$ with respect to some monomial order, every $p \in k[x_1, \ldots, x_n]$ has a unique decomposition

$$p = q + r,$$

where $q \in I$ and no term of r divisible by any $LT(g)$, $g \in G$.

Proposition 10.13

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

(i) For any $p \in k[x_1, \ldots, x_n]$ $\exists!\, r \in k[x_1, \ldots, x_n]$ such that $[p] = [r] \in k[x_1, \ldots, x_n]/I$ and no monomial of r is contained in $\langle LT(I) \rangle$.

(ii) The monomials $\{x^\alpha : x^\alpha \notin \langle LT(I) \rangle\}$ are k-linearly independent modulo I:

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \mod I \Rightarrow \text{all } c_\alpha = 0$$

Proof

(i) Prop 7.8 $\Rightarrow$ unique decomposition $p = q + r$, with $[p] = [q] + [r] = [r]$ and no monomial of r in $\langle LT(I) \rangle$, since $LT(G)$ is by definition a basis of $\langle LT(I) \rangle$.

(ii) $0 \neq \sum c_\alpha x^\alpha \in I \Rightarrow LM(\sum c_\alpha x^\alpha) = x^{\bar{\alpha}}$ divisible by $LT(g) \in \langle LT(I) \rangle$ for some $g \in G$ $\lightning$

Proposition 10.14

Let $I \subset k[x_1, \dots, x_n]$ be an ideal and $G \subset I$ Groebner basis.

For $p \in k[x_1, \dots, x_n]$, denote $\bar{p} = \bar{p}^G$ (remainder of division by G)

Let $S = \text{span}_k\{x^\alpha : x^\alpha \notin \langle LT(I) \rangle\}$

(i) $\varphi : k[x_1, \dots, x_n]/I \to S$, $\varphi([p]) = \bar{p}$

is a k-linear isomorphism.

(ii) $\varphi([p] + [q]) = \bar{p} + \bar{q}$ (follows from (i))

(iii) $\varphi([p] \cdot [q]) = \overline{\bar{p} \cdot \bar{q}}$

Proof

(i) Computing the remainder $p \mapsto \bar{p}$ is k-linear since by uniqueness of the decomposition $p = q + r$

$$\bar{p}_1 = r_1 \ \& \ \bar{p}_2 = r_2 \Rightarrow p_1 = \underset{\in I}{q_1} + r_1 \ \& \ p_2 = \underset{\in I}{q_2} + r_2$$

$$\Rightarrow p_1 + p_2 = \underbrace{(q_1 + q_2)}_{\in I} + (r_1 + r_2)$$

$$\Rightarrow \overline{p_1 + p_2} = r_1 + r_2$$

and similarly for scalar multiples $\overline{cp} = c \cdot \bar{p} \ \forall c \in k$.

Surjectivity follows from $\overline{x^\alpha} = x^\alpha$ for $x^\alpha \in S$.

Injectivity follows from Corollary 7.9:

$$[p] = 0 \iff p \in I \iff \bar{p} = 0 \quad \forall p \in k[x_1, \dots, x_n]$$

(iii) $\varphi([p] \cdot [q]) = \varphi([pq]) = \varphi([\bar{p} \cdot \bar{q}]) = \overline{\bar{p} \cdot \bar{q}}$ $\square$

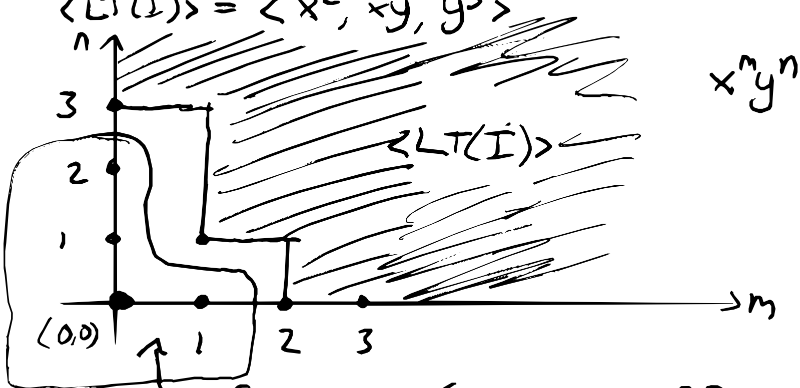
Example 10.15

Let $I = \langle y + x^2 - 1,\ xy - 2y^2 + 2y \rangle \subset \mathbb{R}[x,y]$.

A Grobner basis in lex is

$$G = \{ x^2 + y - 1,\ xy - 2y^2 + 2y,\ y^3 - \tfrac{7}{4}y^2 + \tfrac{3}{4}y \}$$

so $\langle LT(I) \rangle = \langle x^2, xy, y^3 \rangle$



$S = \mathrm{Span}_{\mathbb{R}} \{ 1, x, y, y^2 \}$

Computing products of the $\mathbb{R}$-basis, e.g

$$\overline{x \cdot x} = \overline{x^2} = -y + 1$$

We obtain the multiplication table in S:

1	x	y	y^2
x	$-y+1$	$2y^2 - 2y$	$\frac{3}{2}y^2 - \frac{3}{2}y$
y	$2y^2 - 2y$	y^2	$\frac{7}{4}y^2 - \frac{3}{4}y$
y^2	$\frac{3}{2}y^2 - \frac{3}{2}y$	$\frac{7}{4}y^2 - \frac{3}{4}y$	$\frac{37}{16}y^2 - \frac{21}{16}y$

This describes the ring structure on $\mathbb{R}[x,y]/I$.

Theorem 10.16 (Finiteness Theorem)

Let $I \subset K[x_1 \ldots x_n]$ be an ideal, $G \subset I$ Gröbner basis.

Consider the following statements

(i) $\forall i = 1, \ldots, n \ \exists m_i \geq 0 \quad x_i^{m_i} \in \langle LT(I) \rangle$

(ii) $\forall i = 1, \ldots, n \ \exists m_i \geq 0 \ \exists g \in G \quad x_i^{m_i} = LM(g)$

(iii) The set $\{x^\alpha : x^\alpha \notin \langle LT(I) \rangle\}$ is finite

(iv) $K[x_1 \ldots x_n]/I$ is a finite dimensional K-vectorspace.

(v) $V(I) \subset K^n$ is a finite set.

Then (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv) $\Rightarrow$ (v)

and if K algebraically closed, then also (v) $\Leftrightarrow$ (i)

Proof

(i) $\Rightarrow$ (ii): If $x_i^{m_i} \in \langle LT(I) \rangle$, then $\exists g \in G \quad LT(g) \mid x_i^{m_i}$,

so $LM(g) = x^{\hat{m}_i}$ for some $\hat{m}_i \leq m_i$.

(ii) $\Rightarrow$ (i): $LM(g) = x^{m_i} \in \langle LT(I) \rangle$

(i) $\Rightarrow$ (iii): If $x_i^{m_i} \in \langle LT(I) \rangle$, then all monomials

$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \langle LT(I) \rangle$ if any $\alpha_i \geq m_i$.

Hence $\{x^\alpha : x^\alpha \notin \langle LT(I) \rangle\} \subset \{x^\alpha : \alpha_i \leq m_i - 1 \ \forall i\}$

is finite.

(iii) $\Rightarrow$ (i): If $\{x^\alpha : x^\alpha \notin \langle LT(I) \rangle\}$ has N elements,

then for each i, $\exists m_i \leq N+1$ such that $x_i^{m_i} \in \langle LT(I) \rangle$.

<u>(iii) $\Leftrightarrow$ (iv)</u>: Follows from Prop 10.14, since

$$K[x_1,\dots,x_n]/I \simeq \operatorname{Span}\{x^\alpha : x^\alpha \notin \langle LT(I)\rangle\}$$

as a K-vector space.

<u>(iv) $\Rightarrow$ (v)</u>: Let $N = \dim_K K[x_1,\dots,x_n]/I$. Let $i \in \{1,\dots,n\}$.

Consider the equivalence classes $[x_i^m] \in K[x_1,\dots,x_n]/I$.

$N+1$ of them are K-linearly dependent, so

$$0 = \sum_{m=0}^{N} c_m [x_i^m] = \left[\sum_{m=0}^{N} c_m x_i^m\right]$$

for some $c_0,\dots,c_N \in K$ not all zero.

Hence $p_i = \sum_{m=0}^{N} c_m x_i^m \in I$ and if $a \in V(I) \subset k^n$

then $a_i \in K$ is one of the at most N roots of p.

$$\Rightarrow \# V(I) \le N^n$$

<u>(v) $\Rightarrow$ (i) when K algebraically closed</u>: Let $i \in \{1,\dots,n\}$, $V = V(I)$.

If $V = \emptyset$, then $I = \langle 1\rangle$ by the Weak Nullstellensatz, so $x_i^0 \in \langle LT(I)\rangle$.

If $V \neq \emptyset$, then V finite $\Rightarrow \pi_{x_i}(V)$ finite, where

$$\pi_{x_i} : k^n \to K, \quad \pi_{x_i}(x_1,\dots,x_n) = x_i$$

Let $a_1,\dots,a_m \in K$ be all the points of $\pi_{x_i}(V)$. Define

$$p = (x_i - a_1)\cdots(x_i - a_m) \in K[x_i] \subset K[x_1,\dots,x_n].$$

By construction $p \in I(V)$, so

$$\text{Nullstellensatz} \Rightarrow p \in I(V(I)) = \sqrt{I}$$

$$\Rightarrow p^N \in I \text{ for some } N \in \mathbb{N}$$

$$\Rightarrow LT(p^N) = x_i^{Nm} \in \langle LT(I)\rangle \quad \square$$