CIMPA
Algebraic and Tropical Methods for Solving Differential Equations

Notes by Daniel GCA

June 15, 2023

Contents

1 Tropical Geometry

1.1 Tropical Algebra

Let us define an operation for $a, b \in \mathbb{R}$:

$$a + b = \max\{a, b\}$$

So every element is idempotent, that is, $a + a = a$ for all a. Notice we cannot have a zero element, for there is no element e such that $a + e = a$ for all a. So we must work on the set $\mathbb{T} = \mathbb{R} \cup \{-\infty\}$.

And the product will be ordinary sum:

$$a \cdot b = a + b$$

We must also establish that $a \cdot -\infty = -\infty$ and $(-\infty) \cdot (-\infty) = -\infty$. This makes $(\mathbb{T}, +, \cdot)$ a semiring called the Tropical Semiring.

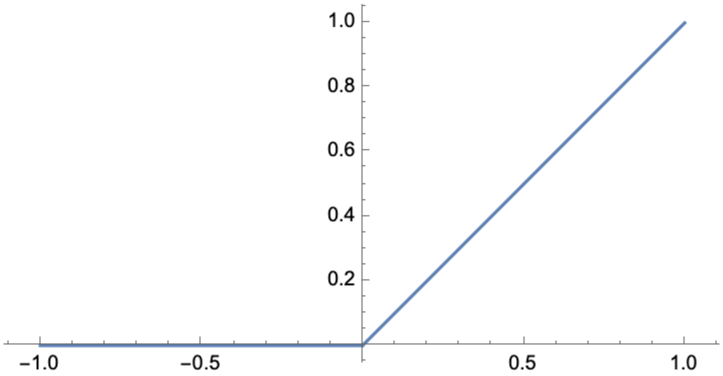
1.2 One variable polynomials

Notice these operations turn usual polynomials into linear equations:

$$\text{“}x^2\text{”} = \text{“}xx\text{”} = 2x$$
$$\text{“}x^2 + y^3\text{”} = \text{“}xxyyy\text{”} = 2x + 3y$$

We write with comas polynomials with usual operations.

Example 1. “$x + 0$” $= \max\{x, 0\}$ is a piecewise linear function with a singularity at 0.



Example 1

Definition (Root)**.** $r \in \mathbb{R}$ is a root of a polynomial f if we can write

$$f(x) = \text{“}\sum_{i=0}^{d} = c_i x^i\text{”} = \max_{i=0}^{d}\{c_i + ix\}$$

and max is reached of at least two monomials. That is, $r \in \mathbb{R}$ is a root if the function defined by f is not lineal in a neighbourhood of r.

Which corresponds to the root 0 of the polynomial in our example.

Example 2. Take the polynomial

$$\text{``}0 + (-1)x + x^2\text{''}$$

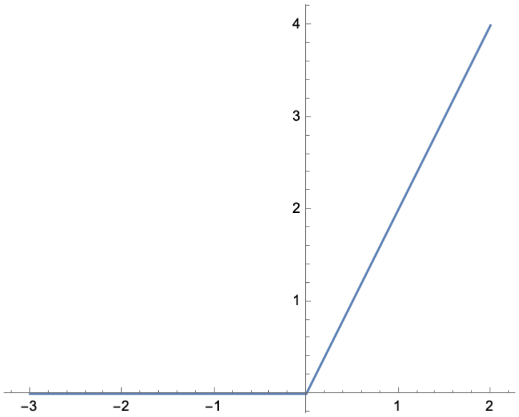


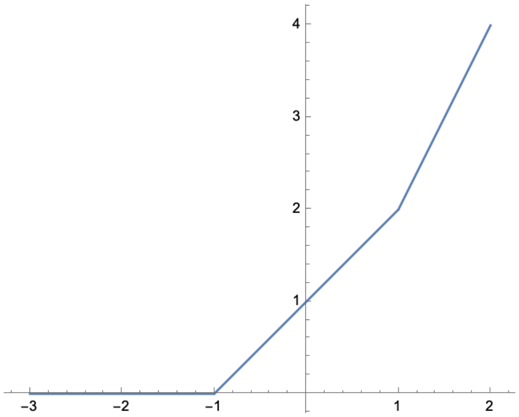
Figure 1

0 is a root of multiplicity 2, for 2 is the distance between the monomials that are not "ghosts" in the polynomial. Only -1 is a ghost coefficient, and the distance between 0 and 2 is 2.

Example 3. Take

$$\text{``}0x + 1 \cdot x + x^2\text{''} = \max\{0, x+1, 2x\}$$

Now we have two singularities, which ammount to two roots, and now both have multiplicity 1.



Example 3

Definition. For $f(x) =$ "$\sum_{i=0}^{d} a_i x^i$" and $x_0 \in \mathbb{R}$, we define

$$\mathrm{In}_{x_0} f(x) = \text{``} \sum_{i \text{ s.t. } f(x_0)=a_i x_0^i} a_i x^i \text{''}$$

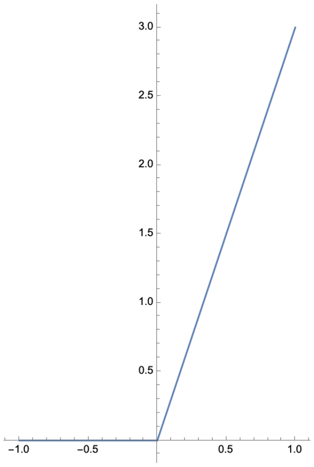
and

$$\mathrm{mult}\ _f(x_0) = \ell(\mathrm{conv}\ \{i : a_i x_0^i = f(x_0)\})$$

Example 4. Take

$$f(x) = \text{``}0 + x + x^2 + x^3\text{''}$$

For $x_0 < 0$ we have $\mathrm{In}_{x_0} f(x) = 0$ and $\mathrm{mult}\ _f(x_0) = 0$. For $x_0 > 0$ we have $\mathrm{In}_{x_0} f(x) =$ "x^3" and $\mathrm{mult}\ _f(x_0) = 0$. And for $x_0 = 0$ we have $\mathrm{In}_{x_0} f(x) = f(x)$ and $\mathrm{mult}\ _f(x_0) = 3$.



Theorem (Fundamental Theorem of Tropical Algebra)**.** For any polynomial of degree d,

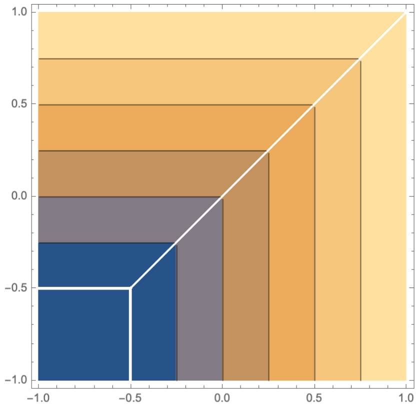
$$\sum_{r \text{ is a root of } f} \text{mult } r = d$$

Thus we now know what is the multiplicity of a root. We must agree that the multiplicity of $-\infty$ is the minimum exponent of the polynomial.

1.3 Two variables

Example 5.

$$f(x,y) = \text{“}0 + x + y\text{”} = \max\{0, x, y\}$$



Definition. For $f(x,y) = \text{“}\sum a_{ij}x^iy^j\text{”}$ define

$$\text{ex}_f = \{(i,j) : a_{ij} \neq 0\}$$

And then the Newton Polygon is

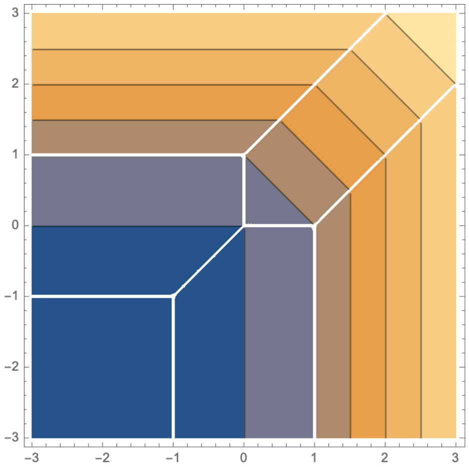
$$\text{conv } \{\text{ex}_f\}$$

So its a vertex for every monomial. And finally:

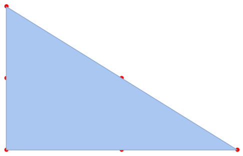
$$C_f := \{(x,y) : \text{In}_{(xy)} f \text{ is not a monomial}\}$$

Example 6. Check this one out:

$$f(x) = \text{“}0 + x + y + xy + x^2 + y^2\text{”} = \max\{0, x+1, y+1, x+y+1, 2x, 2y\}$$



Algebraic curve



Newton polygon

Although the Newton polygon is the dual geometric object of the graph, it cannot be superposed with it because they live in different geometric spaces.

Anyway let's define

Definition. A graph in $\mathbb{R}^2$ is tropical if

1. Edges to rational
2. Weights in the edges
3. Balanced

Definition. Tropical hypersurface defined by f:

$$H_f = \{p : \mathrm{In}_p f \text{ is not a monomial}\}$$

And for an ideal I

$$N_I = \{p : \forall f \in I, \mathrm{In}_p f \text{ is not a monomial}\}$$

1.4 Tropicalization

We will learn how to use tropical geometry to study classical geometry. How can we go from classical polynomial to tropical ones?

Let's take a classical polynomial in $\mathbb{C}[X]$ and induce a tropical polynomial:

$$F(X) = \sum_{i=0}^{d} A_i X^i \rightsquigarrow f(x) = \text{“} \sum_{i=0, A_i \neq 0}^{d} x^i \text{”}$$

It looks to me that you basically get rid of the coefficients and then take the tropical operations.

Now let's try making the coefficients functions of t:

$$F_t(X) = \sum_{i=0}^{d} A_i(t)X^i \rightsquigarrow f(x) = \text{``}\sum_{i=0,A_i\neq 0}^{d} (-\gamma_1)x^{i}\text{''} := F^{\text{trop}}$$

where $A_i(t) = \gamma_j t^j$.

So this time you only take the first coefficient. *Is there anything to correct here?*

Example 7.

$$3t^0 + 4t^0x + x^2 + x^3 + y + t^1xy + x^2y +$$

Theorem 1 (Kaparanov)**.**

$$\begin{tikzcd}
F_t \arrow[r, "\text{zeroes}"] \arrow[d, "\text{tropicalization}"'] & \text{Surface of genus } g \arrow[d, "\text{amoeba: } \mathrm{Log}_t \text{ then } t\to 0"] \\
f \arrow[r, "\text{zeroes}"'] & \begin{array}{c}\text{Tropical curve with}\\ g \text{ bounded regions}\end{array}
\end{tikzcd}$$

And then we can calculate the Newton Polygon and do combinatorics.

1.4.1 Enumerative Geometry

$$N_{\mathbb{C}}(\delta, p) = N_{\mathbb{T}}(\delta, p)$$

1.5 Matroids

Definition (Matroid)**.** $E \neq \emptyset$, B a set of bases that satisfies the Exchange property, that is, for $B_1, B_2 \in B$, there always exists $e_1 \in B_1$ and $e_2 \in B_2$ such that $B_1 \backslash e_1 \cup e_2 \in B$.

Example 8. Let $E = \{a, b, c, d, e\}$ and $B = \{\{a, b, c\}.\{a, b, d\}.\{a, b, e\}, \{a, c, d\}, \{a, c, e\}\}$. For every base lets produce a vector that has 1 if the base contains the element in the corresponding slot according to the order (a, b, c, d, e). So for example the first base has vector $(1, 1, 1, 0, 0)$.

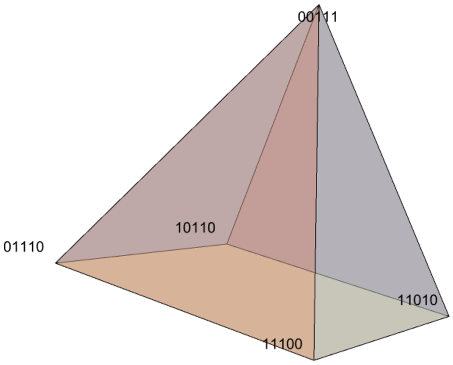
This produces five vectors in $\mathbb{R}^5$ whose convex hull is a polyhedron. Now it turns out that the independent set property lets us direct the edges in this polytope.

Definition. Δ is a matroidal polytope if all the edges of Δ are in direction $e_j - e_i$ for some i, j.

Actually there is a bijection between matroids and these directed polytopes.

Example 9 (Bergman fan, Ardila, Klivans)**.** E of size 5, and a family in $\mathbb{R}^4$. Let us associate:

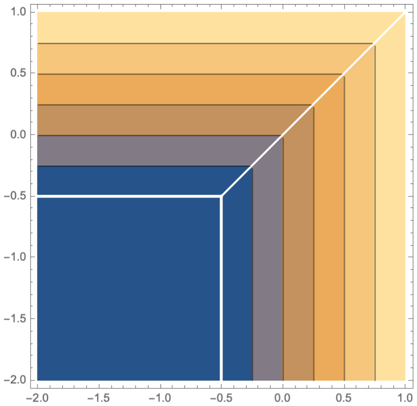
$a \rightsquigarrow (-1, 0, 0, 0)$ $\quad$ $b \rightsquigarrow (0, -1, 0, 0)$ $\quad$ $c \rightsquigarrow (0, 0, -1, 0)$ $\quad$ $d \rightsquigarrow (0, 0, 0, -1)$ $\quad$ $e \rightsquigarrow (1, 1, 1, 1)$



Example 10 (Balanced (Tropical) fan)**.** E of size 3, say $E = \{0, 1, 2\}$ and $B = \{\{0\}, \{1\}, \{2\}\}$. Let us associate:

$$0 \rightsquigarrow (1,1) \qquad 1 \rightsquigarrow (-1,0) \qquad 2 \rightsquigarrow (0,-1)$$

And this produces

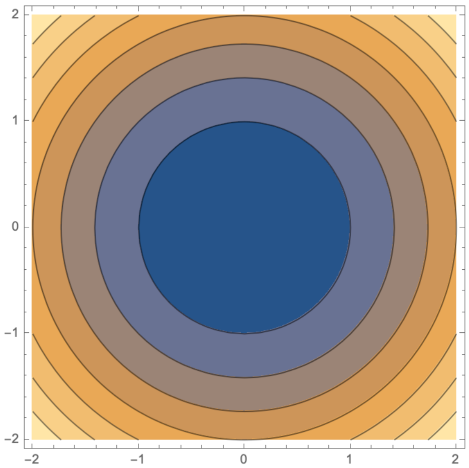


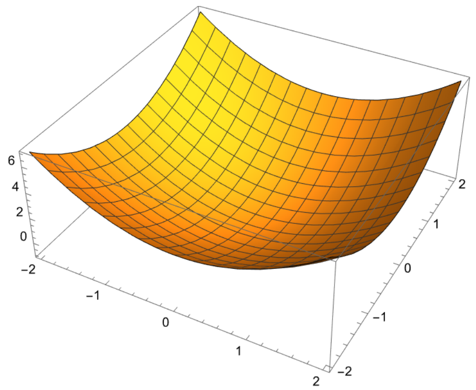
Where every line is a ray spanned by the three vectores we chose. This is the Tropical Fan.

And it turns out matroids are the same as tropical fans of degree 1. And also there's the polytope idea so we have these three definitions. Another example of a tropical fan is the tropical curve in Example 6.

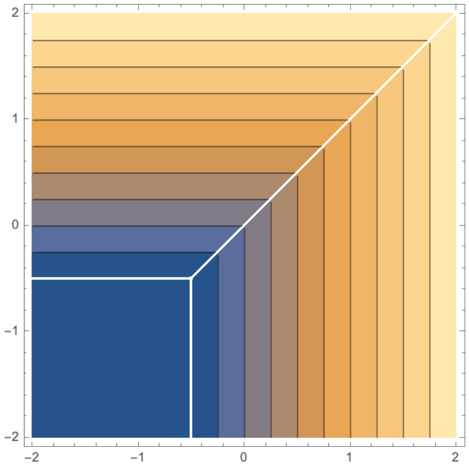
1.6 Dani's three examples

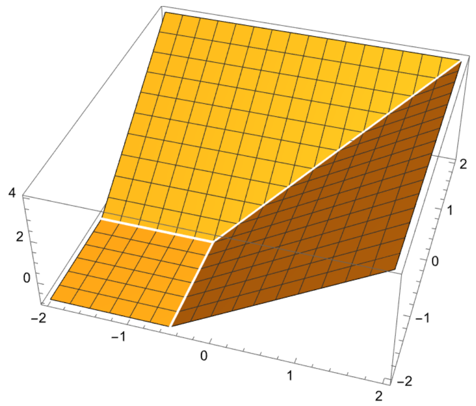
Example 11. Here are the roots of the classical polynomial $x^2 + y^2 - 1$ (with the usual operations in $\mathbb{R}[x, y]$) and its plot in $\mathbb{R}^3$:



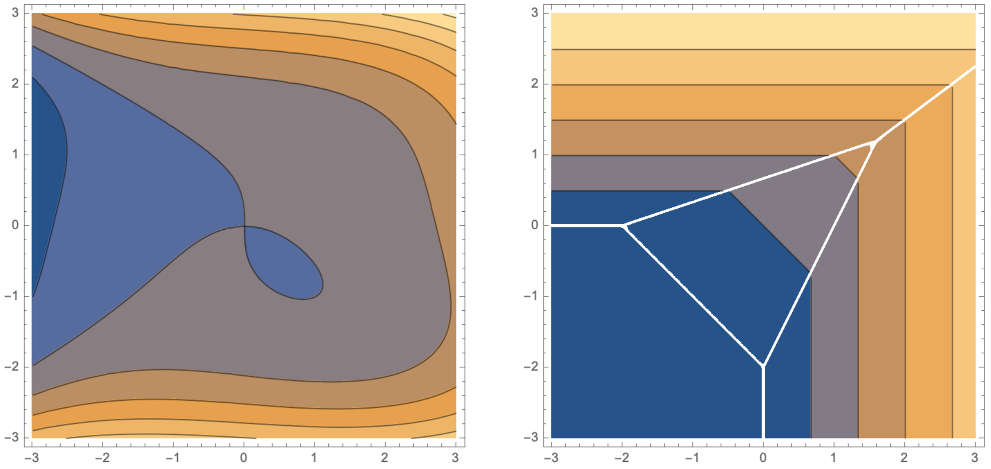


And now we do exactly the same but for the tropical polynomial "$x^2 + y^2 - 1$" $=$ $\max\{2x, 2y, 0\}$:





Example 12. Here are the roots of $x^3 + 2xy + y^4 \in \mathbb{R}[x, y]$ and a related tropical polynomial "$x^3 + 2xy + y^4 + 0$" $= \max\{3x, 2 + x + y, 4y, 0\}$:



Notice we must include the 0 in the tropical polynomial, because without it we do not get the triangle in the plot.

2 Benoit's talk on Real tropical geometry

Let us define a family of polynomials of degree d parametrized by t:

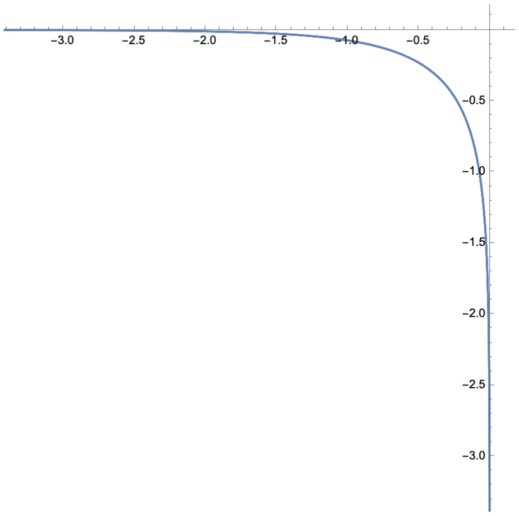
$$p_t(x,y) = \sum_{i+j\leq d} c_{i,j} t^{v_{i,j}} x^i y^j$$

Now consider de map

$$\begin{aligned} \operatorname{Log}_t : (\mathbb{C}^\times)^2 &\to \mathbb{R}^2 \\ (x,y) &\mapsto \Big(\frac{\log|x|}{\log t}, \frac{\log|y|}{\log t}\Big) \end{aligned}$$

And then define for a curve $\mathcal{C} \subset (\mathbb{C}^\times)^2$ the amoeba of $\mathcal{C}$ as $\operatorname{Log}_t(\mathcal{C})$. Notice $\mathcal{C}$ is a *complex* curve, which is a real surface. So the image of our function is a region in $\mathbb{R}^2$.

Here's Dani's incomplete attempt of an amoeba:



And now define as in Lucía's talk:

$$\mathfrak{p} = \text{“}\sum_{i+j\leq d} c_{ij} x^i y^j\text{”} = \max_{i+j\leq d}\{c_{ij} + ix + jy\}$$

Taking edges as perpendicular lines to edges in a tropical conic, and vertices as the centres of regiones determined by the conic, we obtain a subdivision of the plane that looks like the dual tiling of the conic.

Obs. The genus of the curve equals the ammount of bounded regions determined by the tropical curve.

Then he takes the amoebas of the real parts of curves and he obtains plane curves. He then 'unfolds' these curves by taking each part of the curve that is lying in each of the four quadrants of the plane, and then he pastes back each of these pieces.

And then take the limit as $t \to \infty$ and finally folding them back. This is some sort of combinatorial procedure. And it turns out that:

Theorem (Viro, 1976)**.**

$$(\mathbb{R}^2, T_{\mathbb{R}}) \cong (\mathbb{R}^2, \mathcal{C}_{\mathbb{R}})$$

where $\cong$ is homeomorphic. So they have the same Newton polygon and same degree.

Where $T_{\mathbb{R}}$ is the real part he's been working with in the last two paragraphs and $\mathcal{C}_{\mathbb{R}}$ looks like the whole complex curve (real surface).

Example 13 (Dani's attempt to use Benoit's Log function)**.** Let us try to evaluate our Log_t function in a complex algebraic curve. We must remember that the zeroes of polynomials of the form $y^2 = \prod_{k=1}^{2g+1}(x - a_k)$ are called *hyperelliptic curves* when $g > 1$ and *elliptic curves* when $g = 1$ (According to [**diez**]).

Taking $g = 1$, we have a curve of genus 1, that is, a torus. We hope that when we evaluate Log in this torus we get exactly one bounded region in the resulting drawing. The polynomial in this case is

$$y^2 = (x - a_1)(x - a_2)(x - a_3)$$

3 Computational commutative algebra

Matías Bender, matiasbender@inria.fr

3.1 Univariate polynomials and resultants

R a ring, like polynomials. It should be commutative and an integral domain ($a, b \in \mathbb{R} \backslash \{0\} \implies ab \neq 0$). Also take a field $\mathbb{K}$ and its algebraic closure $\bar{\mathbb{K}}$.

3.1.1 Univariate polynomials

Take the polynomial ring $k[x]$ and $f \in k[x]$ with $f = \sum_{i=0}^{d} c_i x^i$ for $c_i \in k$ and $c_d \neq 0$. We say $\deg f = d$.

Now let $k \subseteq \mathbb{K}$ and $p \in \mathbb{K}$ we define $f(p) = \sum_i c_i p^i \in \mathbb{K}$ the evaluation of f. And we say a root of f is p such that $f(p) = 0$.

Question Given $f_1, ..., f_r \in k[x]$, do they have a common root?

Definition. Given $f_1, ..., f_r \in k[x]$ we define the ideal $\langle f_1, ..., f_r \rangle = \{\sum g_i f_i : (g_1, ..., g_r) | ink[x]\}$

Prop. Let $p \in \mathbb{K}$. $\forall f \in \langle f_1, ..., f_r \rangle$, $f(p) = 0 \iff f_i(p) = 0 \forall i$.

Obs. If $g \in \langle f \rangle$, then if $p \in \mathbb{K}$ is such that $f(p) = 0$ then $g(p) = 0$.

Prop. Given $f, g \in k[x]$, there are unique $(q, r) \in k[x]^2$ such that $f = q \cdot g + r$ and $r = 0$ or $\deg r < \deg g$.

We define rem $(f, g) = r$ and write $f | g$ if and only if rem $(f, g) = 0$.

Theorem 2. $k[x]$ is a principal ideal domain. That is, for every ideal $\langle f_1, ..., f_r \rangle$ there exists one polynomial g such that $\langle f_1, ..., f_r \rangle = \langle g \rangle$. g is called GCD of $f_1, ..., f_r$.

I challenge to prove that

Prop. $GCD(f_1, ..., f_r)$ is the smallest polynomial with degree such that if $(\forall i) h | f_i$, then $h | GCD(f_1, ...f_r)$.

Theorem 3 (Euclidean algorithm)**.** Input: $f, g \in k[x]$ with $\deg f \geq \deg g$.

Output: $r \in k[x]$ such that $\langle f, g \rangle = \langle r \rangle$.

Here it goes:

```
$r_{-1} = f, r_0 = g, i = 0$
                $i = i + 1$
                $r_i = \text{rem } (r_{i-2}, r_{i-1})$
        Return $r_{i-1}$
```

Theorem 4. Euclidean Algorithm terminates and is correct.

Proof. It terminates because $\forall i \geq 1)$ $\deg(r_i) > \deg(r_{i+1})$ Hence $\exists i_*$ such that $r_{i_*} = 0$. Observe that for each i, $\exists q_i \in k[x]$ such that $r_{i-2} = r_{i-1}q_i + r_i$. Hence $\langle r_{i-2}, r_{i-1}\rangle = \langle r_{i-1}, r_i\rangle$.
$h_1 r_{i-2} + h_2 r_{i1} \iff (h_1 q_1 + h_2) r_{i-1} + h_i r_i$.
Therefore, $\langle f, g\rangle = \langle r_{-1}, r_0 = ...)\langle r_{k-1}, r_{i_*}\rangle$ □

HW Prove that $GCD(f_1, f_2, f_3) = GCD(GCD(f_1, f_2), f_3)$.

Conclusion If $GDC(f_1, ..., f_r) = 1$, then there are no common solutions.
If $GCD(f_1, ..., f_r) \neq 1$. Then $f_1, ..., f_r$ have ea common factor if $k = \bar{k}$ and $\exists p \in k$ such that $f_1(p) = ... = f_r(p) = 0$.

Now consider a UFD ring R like $\mathbb{C}[y], \mathbb{C}[x, y]$.

Definition (Resultant)**.** Given $f(x, y) = \sum_{i=1}^{m} f_i(y)x^i \in \mathbb{C}[x, y]$ that is, $f \in \mathbb{C}[y]$, and $g = \sum_{i=1}^{m} g_i(y)x^i$. We define Sylvester matrix Sylv (f, g, x).

$$\begin{pmatrix} f_m & 0 & ... & 0 & g_m & 0 & ... & 0 \\ f_{m-1} & f_m & ... & 0 & g_{m-1} & g_m & ... & 0 \\ f_0 & f_1 & ... & 0 & g_0 & g_1 & ... & 0 \\ f_0 & f_0 & ... & f_0 & g_0 & g_0 & ... & g_0 \end{pmatrix}$$

The resultant $Res(f, g, x) = \det \text{Sylv } (f, g, x) \in \mathbb{C}$.

We may substitute $\mathbb{C}$ with any ring R.

Obs. Sylv (f, g, x) represents $\text{Sylv}^{-}{}_{f,g,x}(A, B) \mapsto Af + Bg = \sum c_i x^i$ with $c_i \in \mathbb{R}$. Where $\deg_x(A) < \deg_x(g)$ and $\deg_x(B) < \deg_x(f)$. So A and B are polunomials of the form $A = \sum_{i=0}^{m-1} A_i x^i$ and $B = \sum_{i=1}^{m-1} B_i x^i$. So with two polynomials I obtain another polynomial.

Prop. Res $f, g, x = \text{img Sylv }_{f,g,x}$ that is, $\exists A, B$ such that $\deg A < \deg g$, $\deg B < \deg A$ such that $Af + By = \text{Res } (f, g, x)$.

HW Prove it. Use adjugate matrix of Sylv (f, g, x).

Prop. If $f, g \in k[x]$. The Res $(f, g, x) = 0 \iff GCD(f, g) \neq 1$.

3.1.2 Solving bivariate polynomial systems

Example 14.

$$\text{Sylv } (f, g) = \begin{pmatrix} y & 0 & 2y & 0 \\ y^2 + y & y & 0 & 2y \\ 1 & y^2 + y & -y^2 + 3 & 0 \\ 0 & 1 & 0 & y^2 + 3 \end{pmatrix}$$

Then Res $(f, g, x) = \underbrace{y^2}_{\text{does not lead to a solution}} \quad \underbrace{(2y^2 - 3y - 1)(y + 1)^3}_{\text{lead to solutions!}}$

Theorem 5. If $(p_x, p_y) \in \mathbb{C}^2$ are such that $f(p_x, p_y) = g(p_n, p_y) = 0$ then Res $(f, g, x)|_{y=p_y} = 0$.

Proof. $\exists A, B$ such that $Af + Bg =$ Res $(f, g, x) = 0 =$ Res $(f, g, x)|_{y=p_y}$. □

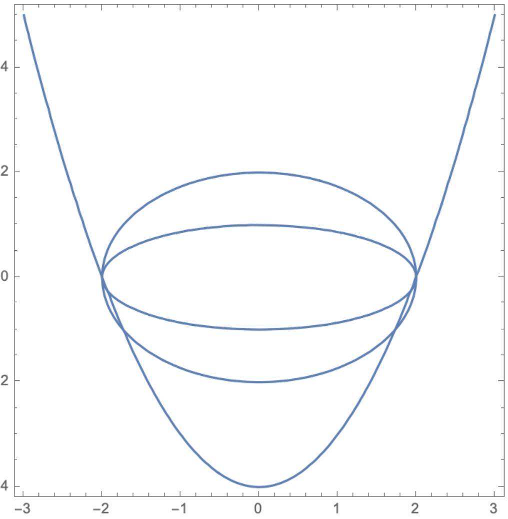
Theorem 6 (Extension theorem)**.** Given $f, g \in \mathbb{C}[x, y]$ as before, let p_y be such that Res $(f, g, x)|_{y=p_y} = 0$. Then if $f_m(p_i) \neq 0$ or $g_m(p_y) \neq 0$, then $\exists p_x$ such that (p_x, p_y) is solution of $f(x, y) = g(x, y) = 0$.

3.2 Ideals and varieties

Example 15. Consider the polynomials

$$\begin{aligned} f_1 &= x^2 + 4y^2 - 4 \\ f_2 &= x^2 + y^2 - 4 \\ f_3 &= x^2 - y - 4 \end{aligned}$$

How can we verify that f_3 vanishes at common zeros of (f_1, f_2)?



Let $R = \mathbb{C}[x_1, ..., x_m]$, $f \in \mathbb{R}$ with $f = \sum_{\alpha \in \mathbb{Z}_{\geq 0}} c_\alpha x^\alpha$ where $c_\alpha \in \mathbb{C}$ there finite α such that $c_\alpha \neq 0$, x^α is monomial , $x^\alpha = \prod_{i=1}^m x_i^{\alpha_i}$.

The degree is $\deg f = \max_{\alpha \in \mathbb{Z}_{\geq 0}}(\sum \alpha_i : c_\alpha \neq 0)$.

Ok now fiven $p \in \mathbb{C}^m$, we can evaluate f doing $f(p) = \sum c_\alpha p^\alpha$. And we say p is a zero if $f(p) = 0$.

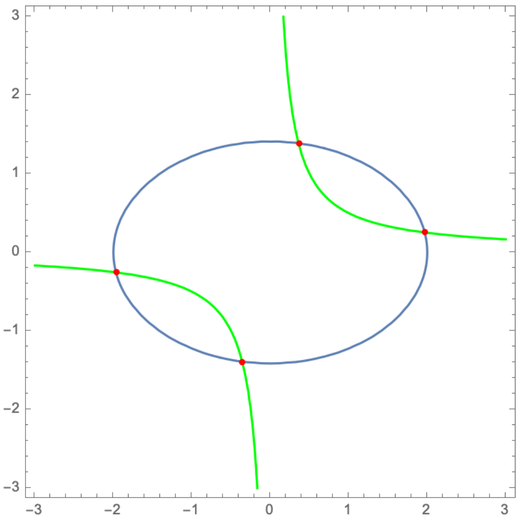
Definition. Given $f_1, ..., f_r \in \mathbb{R}$ we define the affine algebraic variety $V(f_1, ..., f_r) = \{p \in \mathbb{C}^m : (\forall i) f_i(p) = 0\}$. And in general, if $I \subseteq R$ is an ideal, we define

$$V(I) = \{p \in \mathbb{C}^m : (\forall i) f \in I = 0\}$$

.

Example 16. Take

$$\begin{aligned} f_1 &= x^2 + 2y^2 - 4 \\ f_2 &= 2xy - 1 \end{aligned}$$



Definition. An ideal I is a subset of R such that $(\forall f, g \in I) f + g \in I$ and $(\forall f \in I)(\forall r \in \mathbb{R}) fr \in I$.

Prop. Given $f_1, ..., f_r \in R$, we define the generated ideal as

$$\langle f_1, .., f_r \rangle = \{\sum_{i=1}^{r} g_i f_i : g_1, ..., g_r \in R\}$$

Prop. $V(\langle f_1, ..., f_r \rangle) = V(f_1, ..., f_r)$.

Definition. The ring R is Noetherian if when $I \subseteq R$ is an ideal then $\exists f_1, ..., f_r$ such that $I = \langle f_1, ..., f_r \rangle$.

3.2.1 Operations on ideals

Prop. Fix $I, J \subseteq R$ ideals. Then:

1. $I \subseteq J \implies V(J) \subseteq V(I)$
2. $I + J = \{f + g : f \in I, g \in J\}$ is an ideal.
3. $I \cap J$ is an ideal and $V(I \cap J) = V(I) \cup V(J)$.

3.2.2 Hilbert's Nullstellensatz

Definition. Let $W \subseteq \mathbb{C}^n$, we define the ideal

$$I(W) = \{f \in R : (\forall p \in W) f(p) = 0\}$$

.

Prop. Given $W \subseteq \mathbb{C}^n$, $V(W)$ is the smallest with inclusions of the affine algebraic varieties that contain W. If $W \subseteq Z$ and Z variety, then $V(I(W)) \subseteq Z$. Also $\bar{W} = V(I(W))$.

Theorem 7 (Hilbert's Nullstellensatz)**.** Let $I \subseteq R$ be an ideal and $f \in R$. Then, $f \in I(V(I))$ if and only if $f^k \in I$ for some $k \in \mathbb{N}$.

Example 17. This is actually Example 5.

$$\begin{aligned} f_1 &= x^2 + 4y^2 - 4 \\ f_2 &= x^2 + y^2 - 4 \\ f_3 &= x^2 - y - 4 \end{aligned}$$

It turns out that $f_r \notin \langle f_1, f_2 \rangle$. But actually $f_3^2 = (x^2 + \frac{4}{3}y^2 + \frac{2}{3}y - \frac{11}{3})f_1 + (\frac{16}{3}y^2 + \frac{8}{3}y + \frac{1}{2})f_2$ is.

Definition. Given $I \subseteq R$ we define its radical ideal as

$$\sqrt{I} = \{f \in R : (\exists k \in \mathbb{N}) f^k \in I\}$$

Obs. By Hilbert's Nullstellensatz, $\sqrt{I} = I(V(I))$.

Obs. It is necesary that the field we are working on is algebraically closed for Hilbert's Nullstellensatz to be valid.

Corollary 1 (Weak version of Hilbert's Nullstellensatz)**.** $V(I) = \emptyset \iff 1 \in I$

3.2.3 From geometry to algebra

Prop. Given $v, w \in \mathbb{C}^m$ varieties,

1. $I(V \cap W) = \sqrt{I(V) + I(W)}$
2. $I(V \cup W) = I(V) \cap I(W)$
3. Given ideals $I, J \subseteq R$, $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$

3.2.4 Radical membership

Question Given I ideal and f polynomial, does $f \in \sqrt{I}$? Let us introduce a new variable t to define

$$R[t] = \mathbb{C}[x_1, ..., x_n, t]$$

.

Theorem 8. Let $I = \langle f_1, ..., f_r \rangle \subseteq R$. Consider $g \in R$. Then

$$g \in \sqrt{I} \iff 1 \in \langle f_1, ..., f_r, gt - 1 \rangle \subseteq R[t]$$

.

Proof. By Hilbert's Nullstellensatz, $(\forall p \in V(I)) g(p) = 0$. And by Weak Hilbert's Nullstellensatz, $V_{\mathbb{C}^{m+1}}(f_1, ..., f_r, gt - 1) =$. We will prove these two conditions are also equivalent.

We have:

$$(p_1, ..., p_m, p_0) \in V_{\mathbb{C}^{m+1}}(f_1, ..., f_r) \iff \begin{cases} f_1(p_1, ..., p_m) = 0 \\ ... \\ f_r(p_1, ..., p_m) = 0 \\ g(p_1, ..., p_m)p_0 - 1 = 0 \end{cases}$$

The first r equations are equivalent to $(p_1, ..., p_m) \in V_{\mathbb{C}^{m+1}}(f_1, ..., f_r)$. The last equation says $p_0 = \frac{1}{g(p_1, ..., p_m)}$ and that $g(p_1, ..., p_m) \neq 0$.

Anyway we get

$$V_{\mathbb{C}^{m+1}}(f_1, ..., f_r, gt - 1) = \iff (\forall p \in V_{\mathbb{C}^m}(I)) g(p) = 0$$

□

Example 18 (The Rabinowitsch trick, 1929)**.** Use Hilbert's Weak Nullstellensatz to prove Hilbert's Nullstellensatz.

Hint If $(\forall p \in V(I)) g(p) = 0$, then $\exists h_1, ..., h_r, h_0 \in R[t]$ such that $1 = \sum h_i f_i + h_0(gt - 1)$ Replace t by $\frac{1}{g(x_1, ..., x_m)}$ symbolically and clean denominators.

Solution. Let $g \in I(V(I))$ for some ideal $I = \langle f_1, ..., f_r \rangle$, that is, g vanishes whenever all the f_i vanish. Then the polynomials $f_1, ..., f_r, gt - 1$ cannot vanish all at the same time, so that the zeroes of ideal generated by all of them is empty. By Hilbert's Weak Nullstellensatz, this ideal must be the unit ideal (1 is in there). All this is exactly the first phrase in the **Hint**: there must $\exists h_1, ..., h_r, h_0 \in R[t]$ such that $1 = \sum h_i f_i + h_0(gt - 1)$.

When substituting t by $\frac{1}{g(x_1, ..., x_m)}$ we obtain that

$$1 = \sum h_i \Big(\frac{1}{g(x_1, ..., x_m)}, x_1, ..., x_n \Big) f_i \Big(\frac{1}{g(x_1, ..., x_m)}, x_1, ..., x_n \Big)$$

Notice that the expression above is a sum that may have many coefficients of the form $\left(\frac{1}{g(x_1,...,x_m)}\right)^k$. Actually, any denominator on this sum must be of this kind. Thus we can write

$$1 = \frac{\sum h_i(x_1,...,x_n)f_i(x_1,...,x_n)}{g(x_1,...,x_n)^r}$$

for some r which makes $g(x_1,...,x_n)^r$ the common denominator. We have shown $g \in \sqrt{(V(I))}$ □

3.3 Gröbner bases

How can we tell if $f \in I$?

3.3.1 Principal ideals

Remark If $f_1,...,f_r \in \mathbb{C}[x]$, $\exists f_*$ such that $\langle f_1,...,f_r\rangle = \langle f_*\rangle$. Then $g \in \langle f_1,...,f_r\rangle$ (implies?) $f_*|g$.

Remark We should be careful when dividing polynomials of more than one variable (we did a bad example to show this). So we make de following:

3.3.2 Monomial orderings

Definition. A monomial ordering $>$ is a total order for the monomials in R such that

1. $(\forall)x^\alpha \in R\backslash\{1\}$, $1 < x^\alpha$.
2. $(\forall x^\alpha, x^\beta, x^\gamma)x^\alpha < x^\beta \implies x^\gamma x^\alpha < x^\gamma x^\beta$

Prop. If $x^\alpha x^\gamma = x^\beta$ and $x^\gamma \neq 1$, then $x^\alpha < x^\beta$ for any monomial ordering.

Proof. If $1 \neq x^\gamma$, by (1), $1 < x\alpha$. By (2), $x^\alpha = 1x^\alpha < x^\gamma x^\alpha = x^\beta$. □

Definition. The lexicographical monomial ordering $>_{\text{lex}}$ is an ordering such that

$$x^\alpha >_{\text{lex}} x^\beta \iff \exists k \leq m \text{ such that } \alpha_i = \beta_i \text{ for } i < k \text{ and } \alpha_k > \beta_k$$

Example 19.

$$x_1x_2^2x_3 >_{\text{lex}} x_1x_2x_3^{10}$$

Definition. The graded lexicographical monomial ordering $>_{\text{grlex}}$ is an ordering such that

$$x^\alpha >_{\text{grlex}} x^\beta \iff \sum \alpha_i > \sum \beta_i \text{ or } \sum \alpha_i = \sum \beta_i \text{ and } x^\alpha >_{\text{lex}} x^\beta$$

Example 20.

$$x_1^2x_2^2x_3^2 >_{\text{grlex}} x_1^2x_2^3 \quad \text{here we compute deg}$$

$$x_1^2x_2^2x_3^2 >_{\text{grlex}} x_1^2x_2^3x_3 \quad \text{here we use } >_{\text{lex}}$$

Definition. Given $>$ and $f = \sum_{\alpha \in \mathbb{Z}_{\geq 0}} c_\alpha x^\alpha$,

1. **Support.** $\text{supp}(f) = \{x^\alpha : c_\alpha \neq 0\}$
2. **Leading monomial.** $LM_> f = \max_{wrt>}\{x^\alpha \in \text{supp}(f)\}$
3. **Leading coefficient.** $LC_>(f) = c_\alpha$ where $x^\alpha = LM(f)$.
4. **Leading term.** $LT_>(f) = LC_>(f)LM_>(f)$

3.3.3 Polynomial division

Theorem 9 (Division algorithm)**.** Input: $f, g \in k[x]$ and monomial ordering $>$.
Output: $(q, r) \in \mathbb{C}[x_1, ..., x_n]$ such that

1. $g = qf + r$
2. $\forall x \in \text{supp}(r) LM(f) X LM(x)$

$h = g$, $q = 0$, $r = 0$

Here it goes:

```
While ($h \neq 0$)
            If    $LM(f)|LM(h)$
                $q = q + \frac{LT(h)}{LT(f)}$
                $h = h - \frac{LT(h)}{LT(f)}$
        Else
                $r = r + LT(h)$
                $h = h - LT(h)$
Return $(q, r)$
```

HW With one variable, this is the same as the Euclidean algorithm.

Prop. Given $f, g \in R$, $LM_>(f, g) = LM_>(f)LM_>(g)$. In particular, if $g \in \langle f \rangle$, $LM_>(f)LM_>(g) >$ **0?**.

Corollary 2. For some f, g, $g \in \langle f \rangle \iff \text{Rem}(g, f) = 0$

HW Prove this. You have to use the Prop many times.

And then make the division algorithm a little more general:

Theorem 10 (Another Division algorithm)**.** Input: $g, [f_1, ..., f_5] \in k[x]$ and monomial order $>$.
Output: $(q_1, ..., q_s, r) \in \mathbb{C}[x_1, ..., x_n]^{s+1}$ such that

1. $g = \sum q_i f_i + r$
2. $(\forall x^\alpha \in \text{supp}(r))(\forall i \leq s) LM_>(f_i) \nmid x^\alpha$

$\text{Rem}(g, [f_1, ..., f_s], >) = r$

Example 21. Using $>_{\text{lex}}$,

$$f_1 = x^2 + y^2 + y$$
$$f_2 = \underbrace{xy}_{g} + 1$$

Whops! Reminder is $r = 0$.

Prop. Given $f_1, ..., f_s, g \in R$ and $>$, $g - \text{Rem}(g, [f_1, ..., f_s], >) \in \langle f_1, ..., f_3 \rangle$. In particular, if $\text{Rem}(g, [f_1, ..., f_s], >) = 0$, then $g \in \langle f_1, ..., f_s \rangle$

Notice **the opposite does not hold.**

Obs. Given $\langle f_1, ..., f_s \rangle$ we want $\bar{f}_1, ..., \bar{f}_r$ such that $\langle f_1, ..., f_r \rangle = \langle \bar{f}_1, ..., \bar{f}_r \rangle$, $g \in \langle f_1, ..., f_r \rangle \iff \text{Rem}(g, [\bar{f}_1, ..., \bar{f}_r], >) = 0$

Example 22. If $f_1, ..., f_s \in \mathbb{C}[x]$, then $\text{GCD}(f_1, ..., f_r)$ satisfies the property in the Obs.

3.3.4 Gröbner Bases

Definition. Given an ideal I and a monomial ordering $>$, a Gröbner basis (GB) is a set $G \subseteq I$ such that $(\forall g \in I)(\exists f \in G) LM_>(f) LM_>(g)$.

Example 23 (Non-example)**.** $G = [f - 1, ..., f_2]$ is not a GB for $>_{\text{lex}}$ but $-x + y^3 + y = xf_1 - y_f 2$, $LM(f_1)XX$ and $LM(f_2)XX$.

- If $I = \langle f \rangle$ then $[f]$ is a GB I for any monomial ordering.
- If $V(I) =$, by Hilbert's Nullstellensatz then $1 \in I$. If G is a GB of I with respect to, $1 \in I$, so $\exists f \in G$ such that $LM(f)|1$. Hence, $LM(f) = 1$ and then $1 \in G$.

Theorem 11. Every ideal has a finite GB basis with respect to any $>$.

Prop. If G is a finite GB of I with respect to $>$, then $\langle G \rangle = I$.

Proof. Let $g \in I$ and consider $g = \sum q_i f_i + r$ given by division algorithm. Hence, as $g \in I$, $r \in I$. Then another $r = 0$ or $\exists f \in G$. □

Theorem 12. If $[f_1, ..., f_s]$ is a GB of I with respect to $>$, $g\, nI \iff \text{Rem}(g, [f_1, ..., f_s], >) = 0$

Prop. Given $[f_1, ..., f_s]$ and $[\bar{f}_1, ..., \bar{f}_s]$ two GB of I with respect to $>$, then, for any $g \in \mathbb{C}[x_1, ..., x_m]$,

$$\underbrace{\text{Rem}(g, [f_1, ..., f_s])}_{r_1} = \underbrace{\text{Rem}(g, [\bar{f}_1, ..., \bar{f}_s])}_{r_2}$$

Proof.
1. $r_1 - r_2 \in I$ because $g - r_1 \in I$

2. If $r_1 - r_2 \neq 0$, $LM_>(r_1, r_2) \in \mathrm{supp}(r_1) \cup \mathrm{supp}(r_r)$. Wlog, $LM_>(r_1 - r_2) \in \mathrm{supp}(r_1)$. $\mathrm{Rem}(r_1 - r_2, [f_1, ..., f_s], >) = 0$ we get 0. This is a contradiction because $(\forall i \leq s) LM_>(f_1) \nmid LM_>(r_1 - r_2)$.

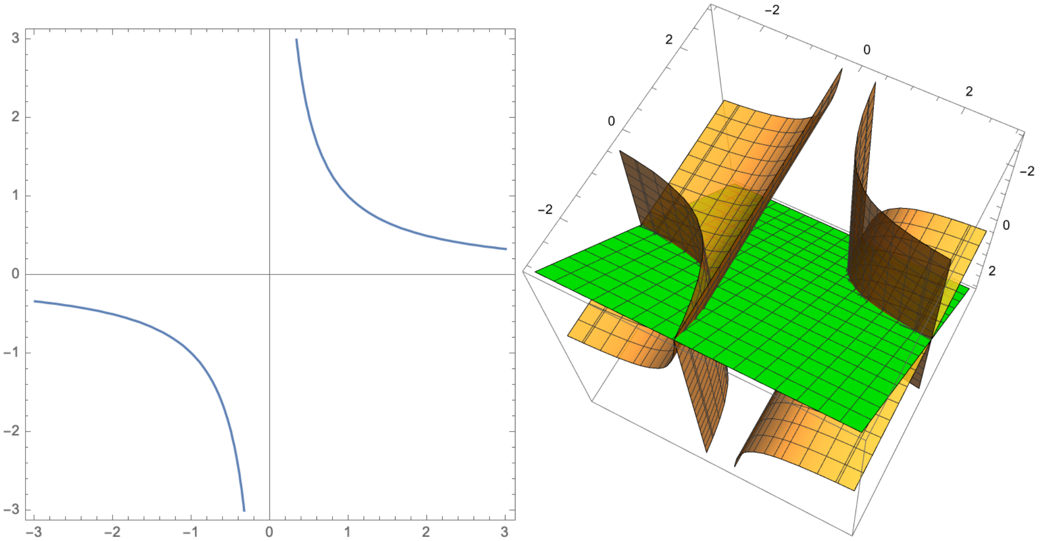
□

3.3.5 Applications of Gröbner Bases

Example 24. Consider

$$f_1 = xy - 1 \qquad \text{and} \qquad f_2 = xz - 1$$

We must try to draw $V(f_1, f_2) \cap \mathbb{R}^3$ and $V(y-1) \cap \mathbb{R}^3$ so as to show the intersection in the green plane $y = z$. Then project $\pi : \mathbb{C}^3 \to \mathbb{C}^2$ with $(p_1, p_2, p_3) \mapsto (p_2, p_3)$ and show $\pi_1(V(f_1, f_2)) = V(y - z) \backslash \{(0, 0)\}$.



Attempt of Figure

3.4 Elimination theory

There's something missing here

Theorem 13 (Extension theorem)**.** $I = \langle f_1, ..., f_s \rangle \subseteq \mathbb{C}[x_1, ..., x_m]$. Let $I_1 = I \cap \mathbb{C}[x_1, ..., x_m]$ we will write f_i as

$$f_i = c_i(x_1, ..., x_m)x_1^{\alpha} + \text{forms of degree } < \alpha_1 \text{ wrt } x <$$

such that $c_i \in \mathbb{C}[x_1, ..., x_r]$ is non zero.

If $(f_1, ..., f_m) \in V_{\mathbb{C}^{m+1}}(I_1) \backslash V_{\mathbb{C}^{m+1}}(c_1, ...c_s)$ then $\exists p_1 \in \mathbb{C}$ such that $(p_1, ..., p_m) \in C(I)$.

Theorem 14 (Closure theorem)**.** $V_{\mathbb{C}^{m-\ell}}(I_\ell) = \overline{\Pi_\ell(V_{\mathbb{C}^m}(I))}$

Theorem 15 (Elimintation theorem)**.** Let G be a GB of I with respect to $>_{\text{lex}}$. Then, $G \cap \mathbb{C}[x_p, ..., x_m]$ is a GB of I with respect to $>_{\text{lex}}$.

Lema. If $LM_{>_{\text{lex}}}(f) \in \mathbb{C}[x_{\ell+1}, ..., x_m]$, then $f \in \mathbb{C}[x_{\ell+1}, ..., x_m]$

> *Proof.* Any monomial x^α involving a variable in $\{x_1, ..., x_\ell\}$ sarisfies $x^\alpha >_{\text{lex}} x^\beta$ for $x^\beta \in \mathbb{C}[x_{\ell+1}, ..., x_m]$. So, if $LM_{>_{\text{lex}}}(f)$ does not involve $\{x_1, ..., x_\ell\}$, no monomial in $\text{supp}(p)$ involves $\{x_1, ..., x_{\ell-1}\}$.

Proof. Consider $f \in I_\ell$ as G is GB, $\exists g \in G$ such that $LM_{>_{\text{lex}}}(g) | LM_{>_{\text{lex}}}(f)$ then $LM_{>_{\text{lex}}} <_{\text{lex}} LM_{>_{\text{lex}}}(f)$, so by the lemma, $g \in \mathbb{C}[x_{\ell+1}, ..., x_m]) \cap G$. □

3.4.1 Saturation of ideals

Definition. Given ideals I, J we define the saturation of I with respect to J as

$$(I : J^\infty) = \{f \in \mathbb{C}[x_1, ..., x_m] | (\forall g \in J)(\exists k \in \mathbb{N}) g^k f \in I\}$$

Example 25.

1. $\langle x(x+1), y(x+1)\rangle : \langle x, y\rangle^\infty = \langle x+1\rangle$
2. $\langle (x-y)xy, (x-y)^3 x^4\rangle : \langle x-y\rangle^\infty = \langle xy, x^3\rangle$

Theorem 16. $V(I : J^\infty) = \overline{V(I)V(J)}$

Theorem 17. Let $I \subseteq \mathbb{C}[x_1, ..., x_m]$ and $g \in \mathbb{C}[x_1, ..., x_m]$. $I : \langle g\rangle^\infty = \langle I, 1 - tg\rangle_{\mathbb{C}[x_1,...,x_m,t]} \cap \mathbb{C}[x_1, ..., x_m]$

Obs. $g \in \sqrt{I} \iff 1 \in \langle I, 1-tg\rangle_{\mathbb{C}[x_1,...,x_m,t]} \iff (I : \langle g\rangle^\infty) \ni 1$

Prop. $(I : (J_1 + J_2)^\infty) = (I_J^\infty) \cap (I : J_2^\infty)$

Corollary 3. If $J = \langle g_1, ..., g_2\rangle$, then $(I : J^\infty) = \bigcap_{i=1}^s (I : \langle g_i\rangle^\infty)$

3.5 Bibliography