Grobner Basis

Friday 14 March 2025 19:31

→ I study Algebraic Geometry.

→ Alg. Geom is about the zeros of polynomals

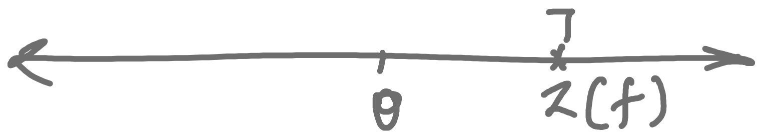
Example When is the function

$$x - 7$$

equal to 0?

ans when $x = 7$.

Geometrically

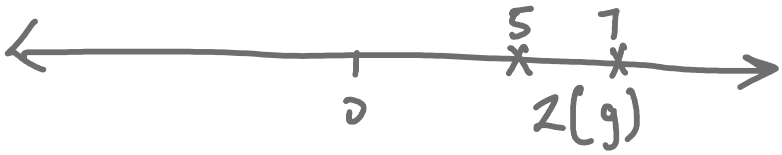


Example When is

$$(x-7)(x-5)$$

equal to 0?

ans when $x = 5$ or $x = 7$.



Notation ① $f = x - 7$; $Z(f) = \{7\}$

② $g = (x-7)(x-5)$; $Z(g) = \{5, 7\}$

* When there is just one unknown, the set of zeros is finite

example $f_1 = x - y$

What is $Z(f_1)$?

we need

$x - y = 0$

So $(x, y) = (1, 1)$ satisfies above condition

$(x, y) = (2, 2)$ satisfies " "

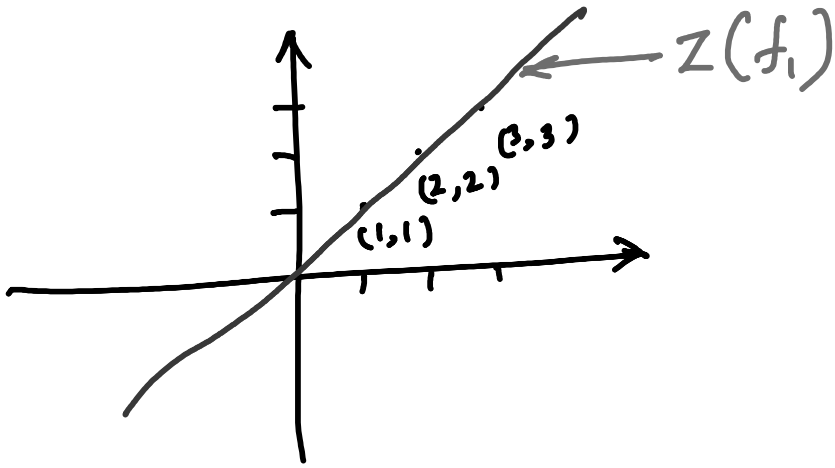
$(x, y) = (3, 3)$ " " "

⋮

all pts of the form (α, α)

for α is a real no. is fine...

$Z(f_1)$:

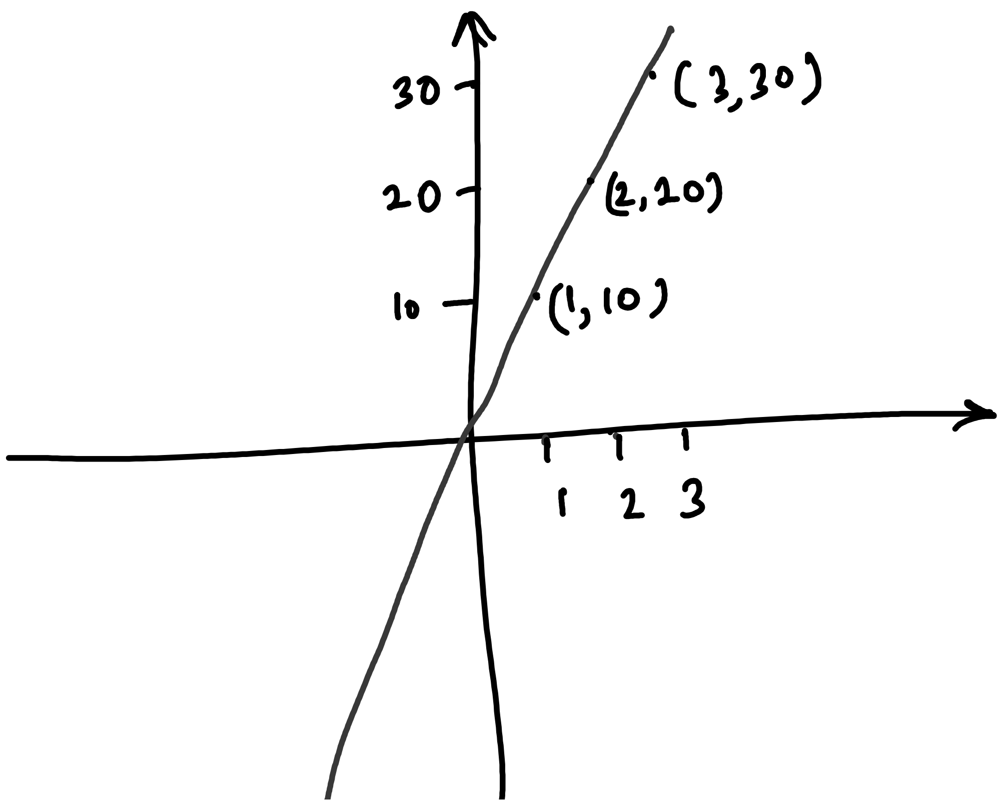


example $f_2 = 10x - y$

$Z(f_2) = ?$

$10x - y = 0$

$(1, 10), (2, 20), (3, 30), (4, 40) \ldots$



$(\quad)$

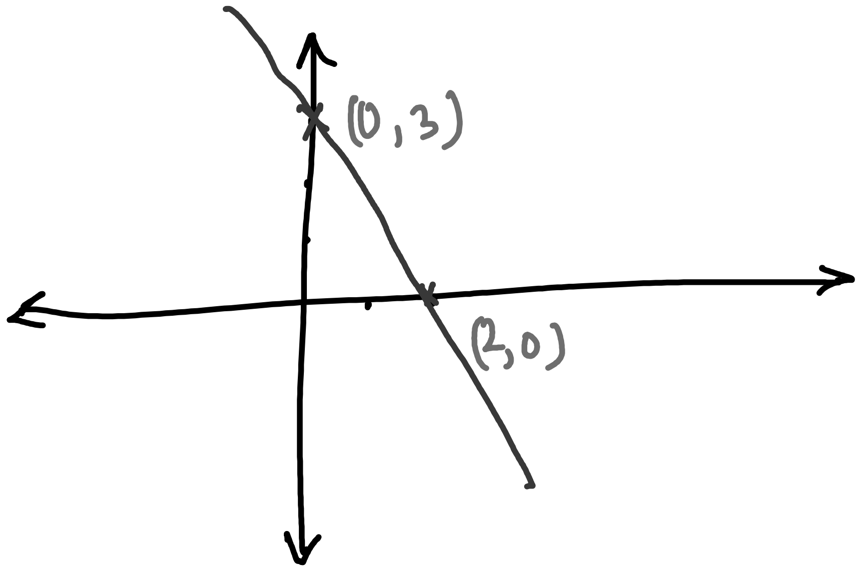
example $f_3 := 2x + 3y - 6$

$Z(f_3)$

$3x + 2y - 6 = 0$

Put $x = 0$ then $y = 3$ $\quad (0,3)$

Put $y = 0$ then $x = 2$ $\quad (2,0)$



Ques Why am I talking about this?

Previous Class, we solved system of linear equations linear equations

example

$$2x - 3y = 5 \leftarrow f$$
$$x + y = 10 \leftarrow g$$

$$\left[\begin{array}{cc|c} 2 & -3 & 5 \\ 1 & 1 & 10 \end{array}\right]$$

$R_2 \leftarrow 2R_2 - R_1$

$$\left[\begin{array}{cc|c} 2 & -3 & 5 \\ 0 & 5 & 15 \end{array}\right]$$

$R_1 \leftarrow 5R_1 + 3R_2$

$$\left[\begin{array}{cc|c} 10 & 0 & 70 \\ 0 & 5 & 15 \end{array}\right]$$

$R_1 \leftarrow \frac{R_1}{10}$; $R_2 \leftarrow \frac{R_2}{5}$

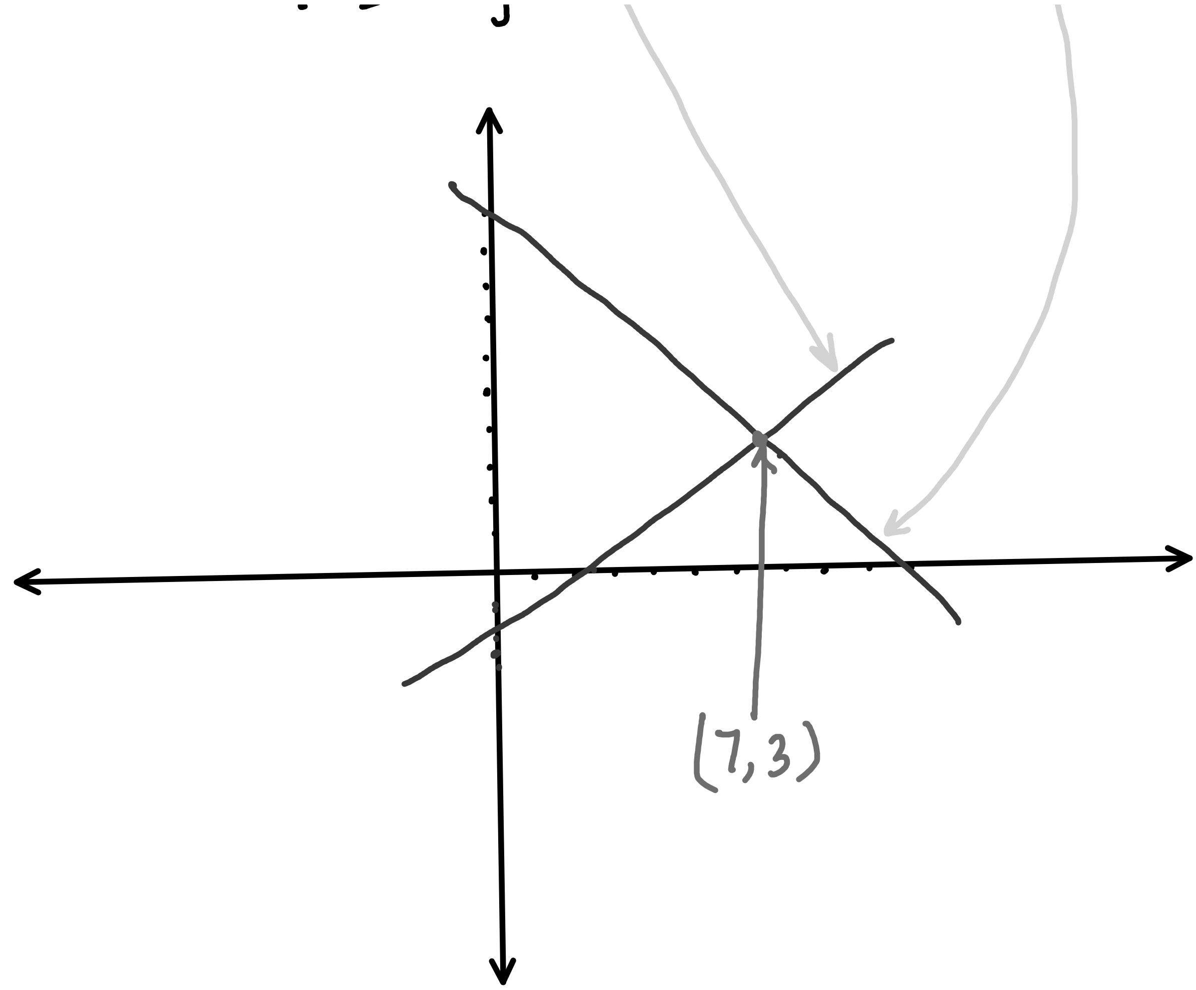
$$\left[\begin{array}{cc|c} 1 & 0 & 7 \\ 0 & 1 & 3 \end{array}\right] \Rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 \\ 3 \end{bmatrix}$$

$2x - 3y = 5$

$\Rightarrow 2x - 3y - 5 = 0$

$x + y = 10$

$x + y - 10 = 0$



Solving system of linear equations ☆ $f_1 \ldots f_n$ is equivalent to finding $Z(f_1), \ldots, Z(f_n)$ and finding the point common to all $Z(f_1) \ldots Z(f_n)$ ☆

<u>Defn</u> [Monomial] given variables x, y, z, w.

a monomial is $x^{c_1} y^{c_2} z^{c_3} w^{c_4}$

where $c_1, \ldots, c_4$ are all non-negative integers e.g. x^2, $x^2 y$, $x y^2 z$, .

Defn [Polynomial] Sum of scalar multiples of monomials.

e.g. $x^2 + y$, $x + y$, $4x - 5y^2$, $3z^2 y + 15y^2 - 2z$, ...

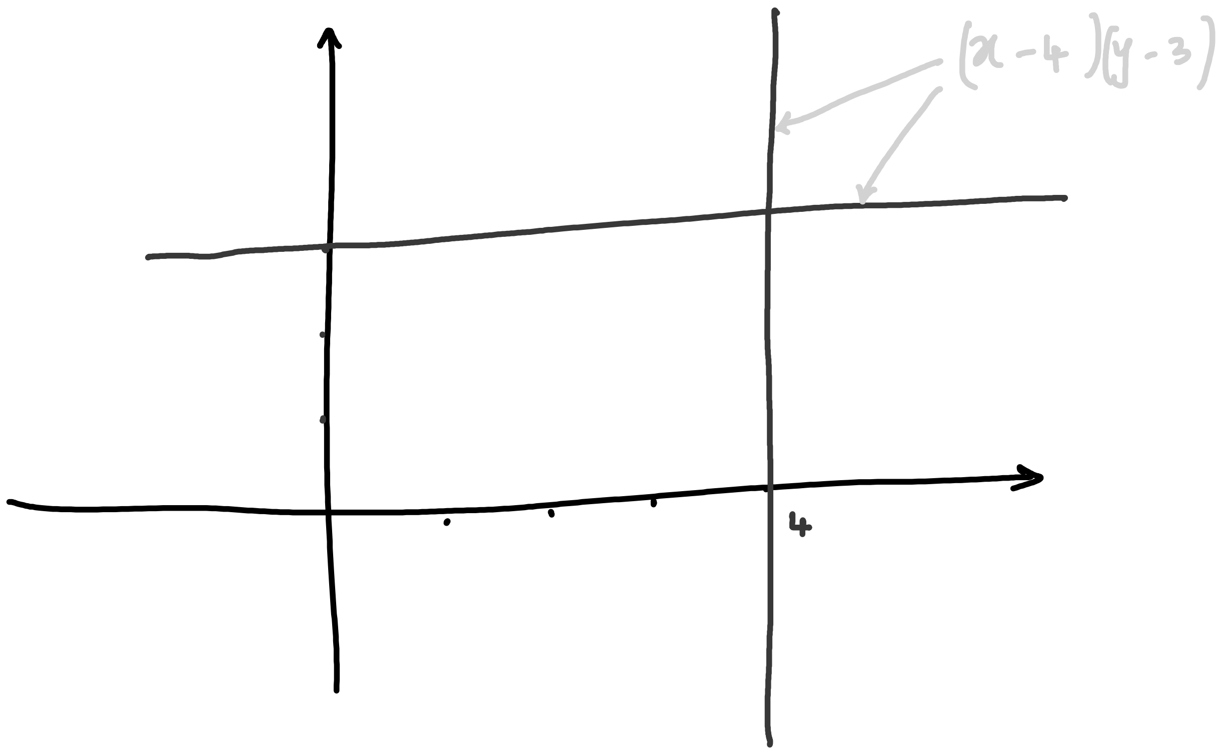
Question At what pts. is a polynomial equal to zero?

Example $(x-4)(x-3)$

This is zero when $x = 4$ or $x = 3$

example $(x-4)(y-3)$

This is zero when $x = 4$ or $y = 3$

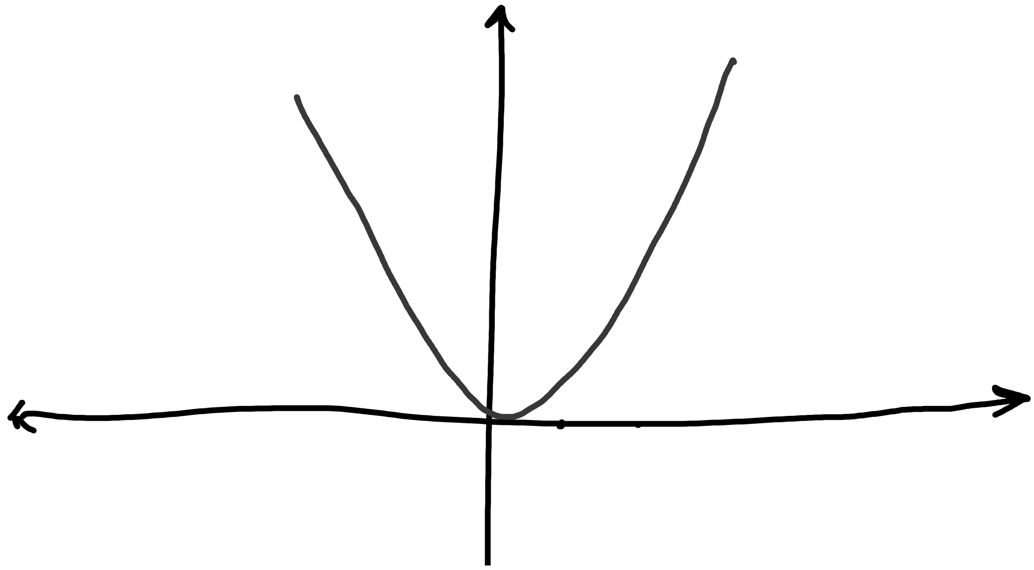


<u>Example</u> $x^2 - y$

This is zero when $y = x^2$

$(0,0), (1,1), (2,4), (3,9), (4,16)$

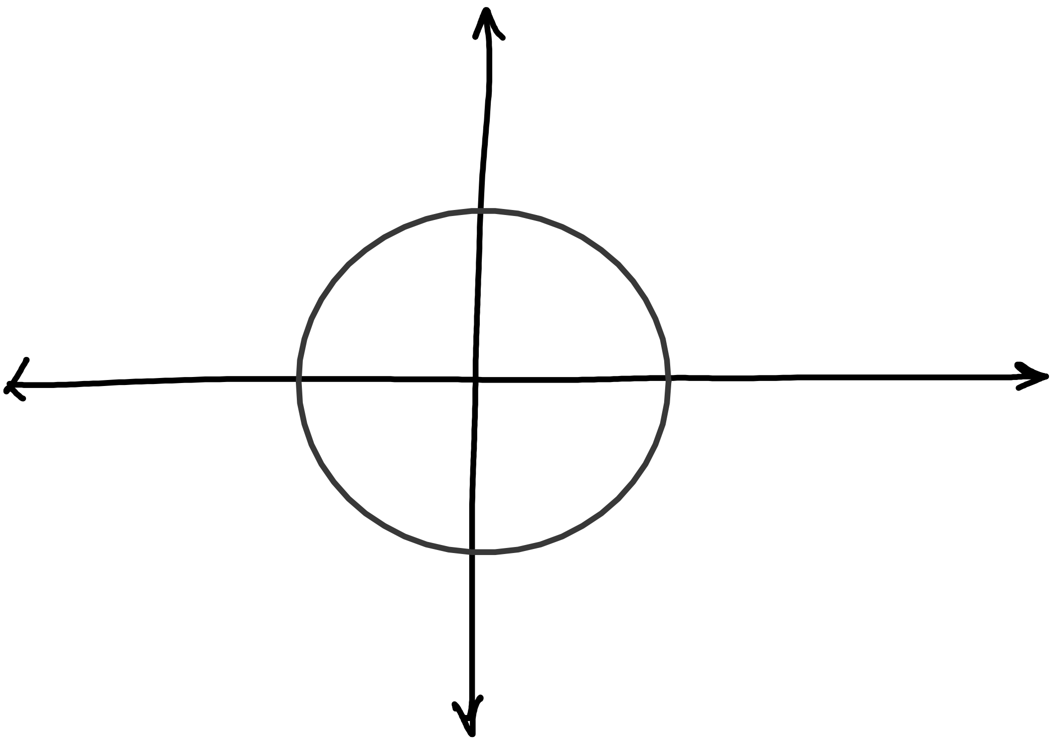
$(-1,1), (-2,4), (-3,9), \ldots$



example

$$x^2 + y^2 - 4$$

This is zero when pts. lie on a circle



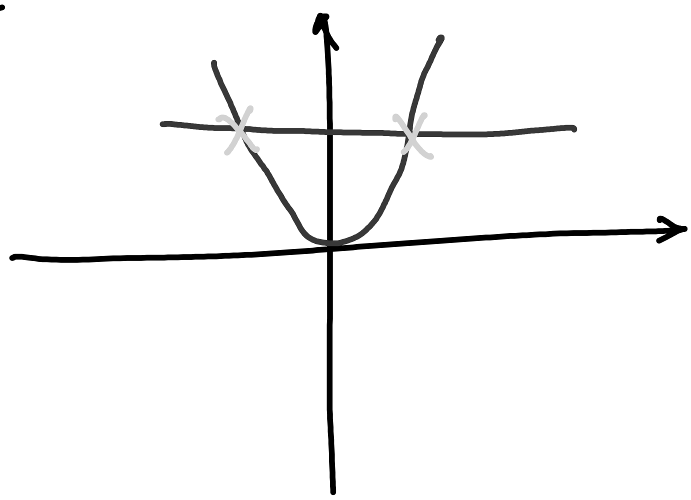
Homework Plot the zeros of

$$\frac{x^2}{2} + \frac{y^2}{3} - 1 .$$

Question Solve the system.

$$y = 4$$
$$y = x^2$$

Ans. 1



Ans 2 $\quad y = 4$ & $y = x^2$

$$\Rightarrow x^2 = 4$$

$$\Rightarrow (x-2)(x+2) = 0$$

$$\Rightarrow \boxed{\begin{matrix} x = 2 \\ y = 4 \end{matrix}} \text{ or } \boxed{\begin{matrix} x = -2 \\ y = 4 \end{matrix}}$$

The key to solving the previous example was being able to

→ do $y = x^2$ and then substitute

do $y = x^2$ and then substitute

→ Suppose you have $x^5 + y^5 + x + y - 4 = 0$, you cannot express either x or y in terms of the others

Homework Google "unsolvability of quintic" and just read any result

We can't do anything about the above example, but we need a method to solve a system of polynomial eqns.

Recall how we solve linear eqns

$$7 \times (3x + y = -1)$$
$$- \quad 3 \times (7x + 11y = 15)$$
$$= \quad -26y = -52$$

Thus $y = 2$, $x = -1$.

Gaussian elim is just the above step repeated often

Question Can we do the above for a system of polynomials?

example

$$x \times \left(x^2 y^3 - 256 = 0 \right)$$

$-$

$$y \times \left(x^3 y^2 - 128 = 0 \right)$$

need to make the leading monomial the same

$$-256x + 128y = 0$$

$$\Rightarrow \boxed{y = 2x}$$

Back substitution gives

Back substitution gives

$$\boxed{x=2,\ y=4}$$

---

example

$$xy-1$$
$$x+y-2$$

$$xy-1$$
$$-x(y+x-2)$$

$$(xy-1)-(xy+x^2-2x)$$

$$= -1-x^2+2x$$

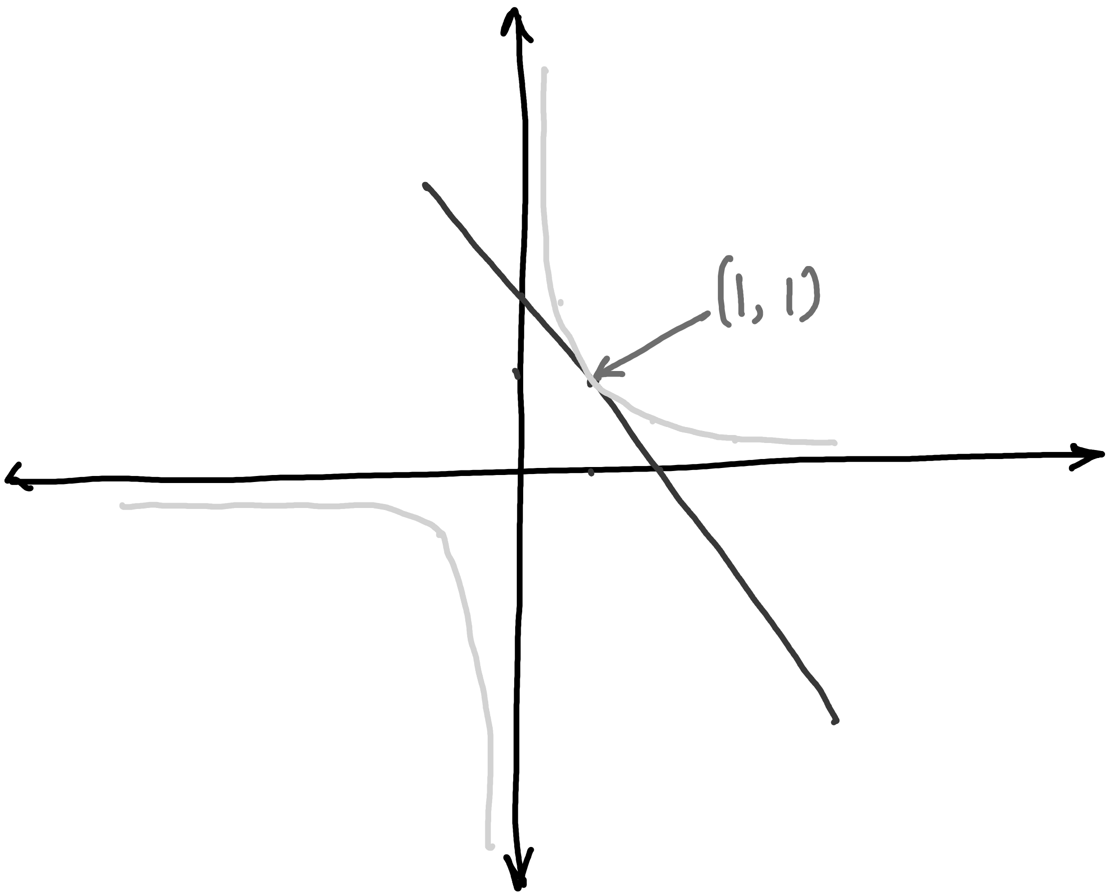
$$=0$$

$$(x^2-2x+1)=0 \iff (x-1)^2=0$$

$$\Rightarrow x=1$$

Substitute $x=1$ in $x+y-2$

gives $y = 1$



Algorithm [Modified Gaussian Elimination for system of polynomials]

Step 1 Given system of polynomials G, eliminate leading term of every pair of polynomials

e.g.

$\{x\ y^2 \qquad \}$

e.g.

$$z\left(xy^2 + \cdots\right)$$

$$x\left(y^2z + \cdots\right)$$

$$\begin{array}{r} xy^2z \;\cdots \\ -\; xy^2z \;\cdots \\ \hline = \;0 \;\cdots \end{array}$$

Step 2 Do until the system becomes easy to solve.

Defn [S-polynomial] Given polynomials f and g, the polynomial formed by eliminating the leading terms is by eliminating the leading terms is called the S-polynomial of f and g, denoted $S(f,g)$.

Defn [Gröbner Basis] The set of all polynomials and S-polynomials is called the Gröbner Basis of the original system.

<u>example</u>

$$f_1 = xy - z$$

$$f_2 = xz - y$$

$$f_3 = yz - x$$

$$S(f_1, f_2) = z(xy - z) - y(xz - y)$$

$$= y^2 - z^2$$

$$S(f_1, f_3) = z(xy - z)$$

$$S(f_1, f_3) = z(xy - z)$$
$$\quad - x(yz - x)$$
$$= x^2 - y^2$$
$$S(f_2, f_3) = y(xz - y)$$
$$\quad - x(yz - x)$$
$$= x^2 - y^2$$

Thus we could equivalently look at

$$x^2 - y^2 = 0, \quad x^2 - z^2 = 0, \quad y^2 - z^2 = 0$$
$$x^2 = y^2 \qquad x^2 = z^2 \qquad y^2 = z^2$$

thus $\boxed{x^2 = y^2 = z^2}$

To solve the system, we consider

$(x, y, z) = (\pm t, \pm t, \pm t)$ for

any t. Also

$xy = z \quad x = yz, \quad y = xz$

Substituting $*$, we get

$\pm t^2 = + t$ in all three eqns.

The only thing that satisfies all three eqns is $t = 0$ or $t = 1$

Thus the only solutions are $(0,0,0)$ or $(1,1,1)$.

Possible with the mechanical Procedure of Grobner Bases.

The algorithm is called

Buchberger's Algorithm

Exercise

exercise

$$f_1 = x^2 + y^2 - 1$$
$$f_2 = x^2 + z^2 - 1$$
$$f_3 = y + z$$

$$g_1 := S(f_1, f_2) =$$
$$\begin{aligned} & 1\,(x^2 + y^2 - 1) \\ - & 1\,(x^2 + z^2 - 1) \end{aligned}$$

$$= y^2 - z^2$$

$$g_2 = S(f_1, f_3)$$

$$= \begin{aligned} & y\,(x^2 + y^2 - 1) \\ - & x^2\,(y + z) \end{aligned}$$

$$= y^3 - x^2 z - 1$$

$g_3 = S(f_2, f_3)$

$$y\left(x^2 + z^2 - 1\right)$$

$$x^2\left(y + z\right)$$

$$= yz^2 - x^2 z - 1$$

g_2 and g_3 don't seem useful.

g_1 looks good, but not enough to solve, so LETS CONTINUE

$h_1 = S(g_1, f_3)$

$$= y^2 - z^2$$

$y\,(y+z)$

$= yz - z^2$

$yz - z^2 = 0 \Rightarrow z(y-z)=0$

① $z=0$

$\Rightarrow y=0$ (bcoz $y^2 - z^2 = 0$)

$\Rightarrow x = \pm 1$

② $y=z$

put in f_3 to get

$2z=0 \Rightarrow z=0$

!! same as above !!

Thus the solutions are

$(1,0,0)$ and $(-1,0,0)$ ✓

• Polynomial division

Ques: divide $x^3+2x^2+\cancel{48}\,4x+8$ by $x+2$

$$\begin{array}{r l}
 & x^2+4 \\ \hline
x+2 \,\big) & x^3+2x^2+4x+8 \\
 & \underline{x^3+2x^2} \\
 & 0+4x+8 \\
 & \underline{4x+8} \\
 & 0
\end{array}$$

Check $(x+2)(x^2+4)$

Example: divide $(x^5-8x^4+13x^3+7x^2-32x+10)$ by (x^2-6x+2)

$$\begin{array}{r l}
 & x^3-2x^2-x+5 \\ \hline
x^2-6x+2 \,\big) & x^5-8x^4+13x^3+7x^2-32x+10 \\
 & \underline{x^5-6x^4+2x^3} \\
 & -2x^4+11x^3+7x^2 \\
 & \underline{-2x^4+12x^3-4x^2} \\
 & -x^3+11x^2-32x \\
 & \underline{-x^3+6x^2-2x} \\
 & 5x^2-30x+10 \\
 & \underline{5x^2-30x+10} \\
 & 0
\end{array}$$

Generalization of division??

→ divide 32 by 5

$$32 = 5 \times \underbrace{6}_{\text{quotient}} + \underbrace{2}_{\text{remainder}}$$

→ divide 32 by (6, 4)
what I mean is

$$32 = 6 \times \underbrace{4}_{\text{quotient 1}} + 4 \times \underbrace{2}_{\text{quotient 2}} + \underbrace{0}_{\text{remainder}}$$

→ divide 32 by (5, 7)

negative quotient!

$$32 = 5 \times \underbrace{12}_{\text{quotient 1}} + 7 \times \underbrace{(-4)}_{\text{quotient 2}} + \underbrace{0}_{\text{remainder}}$$

Ex homework: any positive or negative no. can be divided by the pair (13, 7)! YES! Prove it!

Same thing gets very awkward with Polynomial division!

→ divide xy^2+1 by $f_1 = xy+1$ & $f_2 = y+1$

q_1 : y
q_2 : -1

$$\begin{array}{l|l} f_1 \;\; xy+1 & xy^2+1 \\ f_2 \;\; y+1 & xy^2+y \\ \hline & -y+1 \\ & -y-1 \\ \hline & \quad 2 \end{array}$$

$$\therefore (xy^2+1) = (xy+1)\times \underbrace{y}_{\text{quotient 1}} + (y+1)\underbrace{(-1)}_{\text{quotient 2}} + \underbrace{2}_{\text{remainder}}$$

→ divide $x^2y+xy^2+y^2$ by $f_1 = xy-1$ and $f_2 = y^2-1$

$q_1 : x+y$
$q_2 : 1$

$$\begin{array}{l|l} f_1 = xy-1 & x^2y+xy^2+y^2 \\ f_2 = y^2-1 & x^2y-x \\ \hline & xy^2+x+y^2 \\ & xy^2-y \\ \hline & \cancel{x}+y^2+y \\ & y^2-1 \\ \hline & y+1 \end{array}$$

remainder
$x+y+1$

Thus:

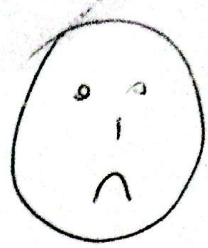
$$(x^2y+xy^2+y^2) = (xy-1)\times\underbrace{(x+y)}_{\text{Quot 1}} + (y^2-1)\times\underbrace{(1)}_{\text{Quot 2}} + \underbrace{x+y+1}_{\text{remainder}}$$

- Previous ~~method~~ exercise was awkward …

"Can you divide"

→ ~~divide~~ $16x^2 - 12xy$ by $f_1 = x^2y - 9x - 3$, $f_2 = xy^2 - 9y - 4$.

$$\begin{array}{l|l} x^2y - 9x - 3 & \overline{16x^2 - 12xy} \\ xy^2 - 9y - 4 & \end{array} \quad \ldots$$



<u>Solution</u> find Grob. basis of (f_1, f_2)

$$S(f_1, f_2) = y \times f_1 - x \times f_2$$
$$= 4x - 3y.$$

$$\begin{array}{r|l} & \quad 4x \\ 4x - 3y & \overline{16x^2 - 12xy} \\ & \underline{16x^2 - 12xy} \\ & \qquad 0 \end{array}$$

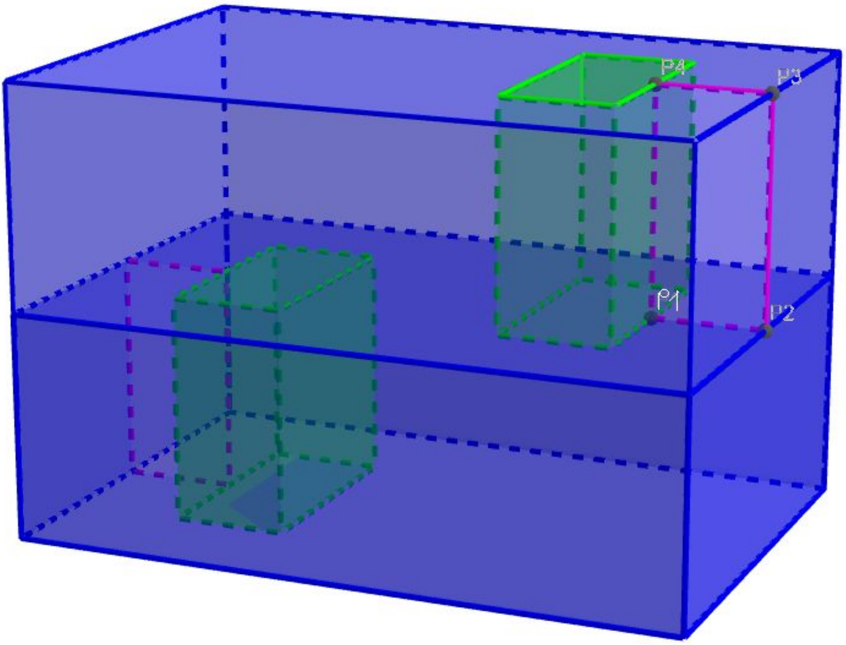
<u>Thm</u> divisibility by $f_1 \ldots f_2$ $\stackrel{\text{equivalent to}}{\Longleftrightarrow}$ divisibility by Grob-basis of $f_1 \ldots f_2$

Thus YOU CAN INDEED DIVIDE $16x^2 - 12xy$ by f_1 & f_2

Topology

→ Study of objects that remain the same on bending, stretching, etc.

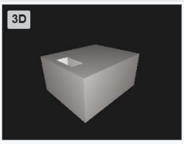
CamScanner



House with two rooms

From Wikipedia, the free encyclopedia

House with two rooms or **Bing's house** is a particular contractible, 2-dimensional simplicial complex that is not collapsible. The name was given by R. H. Bing.[1]


3D

A 3D model of Bing's house

The house is made of 2-dimensional panels, and has two rooms. The upper room may be entered from the bottom face, while the lower room may be entered from the upper face. There are two small panels attached to the tunnels between the rooms, which make this simplicial complex contractible.

See also [edit]

- Dogbone space
- Dunce hat

Comes down to Counting holes

"Betti Numbers"

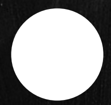
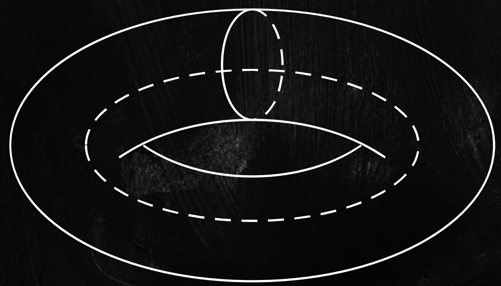
(b_0) (Zeroth Betti number) - no. of connected pieces

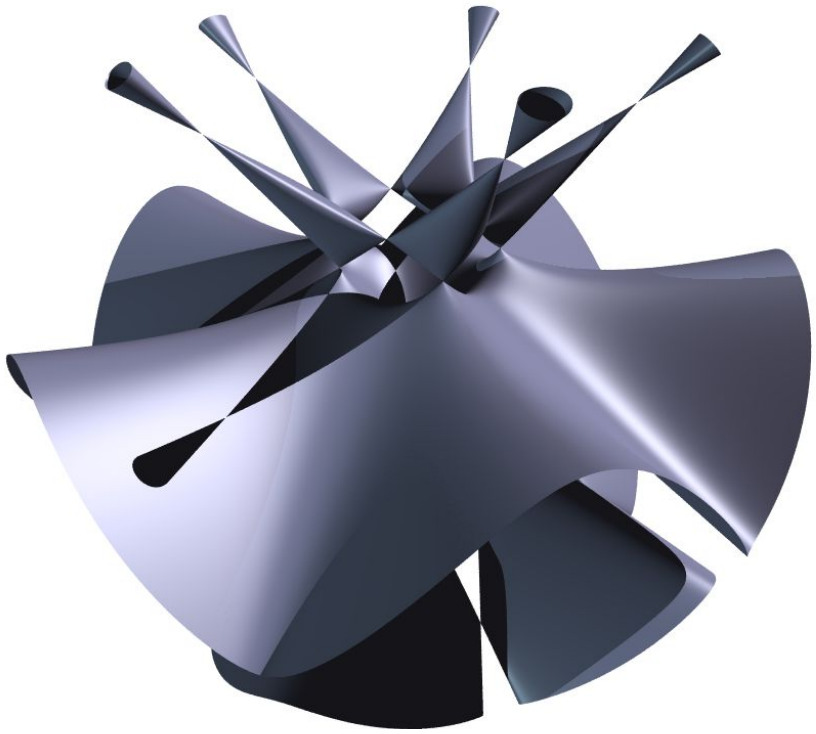
(b_1) ($\underline{1}^{st}$ Betti no.) - no of 1-d holes

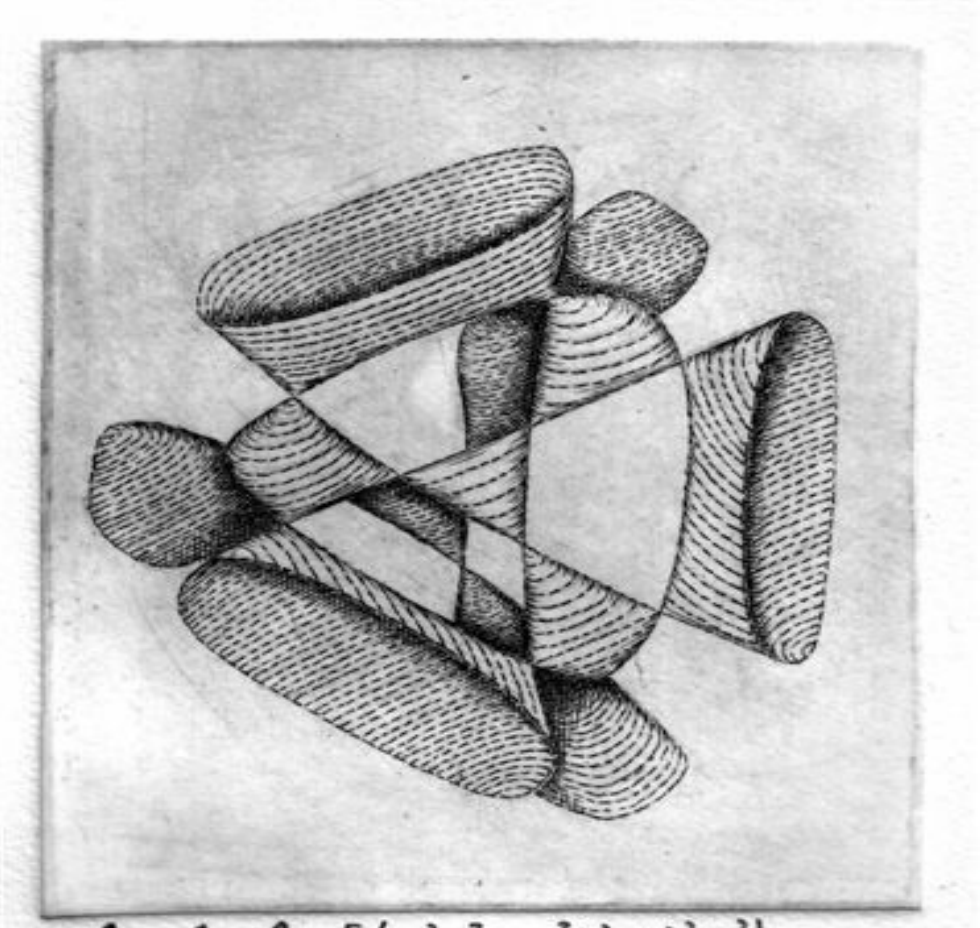
(b_2) (2^{nd} Betti No.) - no. of 2-d holes

⋮

Betti Numbers – Examples

Object	b_0	b_1	b_2	$b_{i\geqslant 3}$
•	1	0	0	0
• • • • •	5	0	0	0
	1	1	0	0
	1	0	0	0
	1	0	1	0
	1	2	1	0





$$x^4+y^4+z^4-5(x^2y^2+y^2z^2+z^2x^2)$$
$$+56xyz-20(x^2+y^2+z^2)+16=0$$

Zero knowledge proofs

- Prover (P)
- Verifier (V)

P can convince V that something is true without V knowing anything beyond the fact that it is true

non-example 'P' claims there is an integer x such that

$$x^3 = 8$$

'V' - Show ~~ke~~ me how!

'P' - says try $x = 2$

'V' - is convinced!

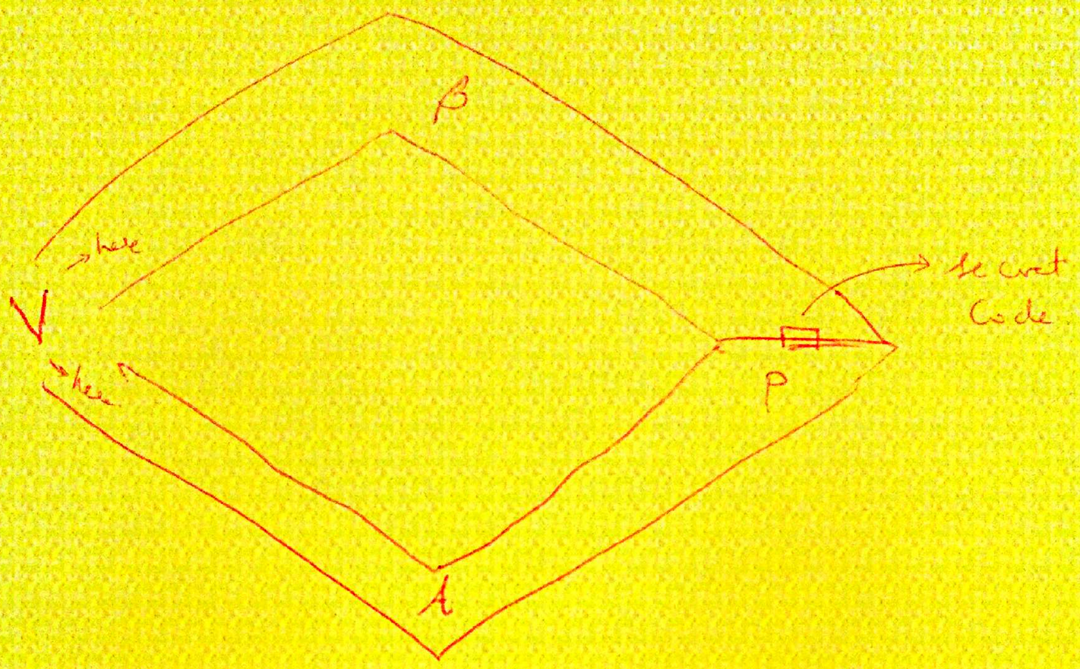
e.g 'P' claims I'm not colour blind.

'V' - who is blind folded needs to ~~take~~ be convinced.

'V' takes 2 balls, red (R) & Blue (B)

- Swap or no swap behind back & show
- 'P' must guess yes or no.

After many times 'V' must be convinced.



P goes in via 'A' or 'B' unknown to ~~[illegible]~~ V

V calls out – "come via 'B'" or "come via A"

P must be successful all time.

Prob of falsely convinced after 'n' tries is

$$\frac{1}{2^n}$$

$n - 20$ Prob of hallucinating