MAG Lecture 1 : What is Algebraic Geometry?

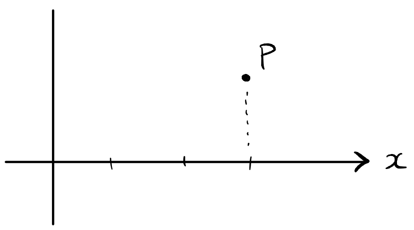
Algebraic geometry is the study of curves, surfaces and higher-dimensional objects defined by polynomial equations. It is the home of one of the deepest ideas in mathematics, the duality between

Spaces	and	Functions
X		$f : X \longrightarrow \mathbb{C}$
things		measurements
curves, surfaces, ...		polynomials, ideals, ...
geometry		algebra
?		computation / algorithms

We will develop this duality over 8 weeks, following D. Cox, J. Little and D. O'Shea "Ideals, Varieties and Algorithms" 4th edition (here CLO). The aim is to reach the Elimination Theorem, which is a good illustration of the power of algebraic (and computational) techniques to solve geometric problems. Along the way we will see topics including Gröbner bases, the Hilbert basis theorem, and Buchberger's algorithm.

References to CLO look like: Section 1.2, or §1.2, meaning Section 2 of Chapter 1, and Lemma 1.2.2 meaning Lemma 2 in Section 1.2.

From childhood we are exposed to the idea of space being imbued with a coordinate system, and we learn to associate the letters x, y, z with the coordinate functions. We say coordinate functions because x is not a real number, but the "measurement" of a point's "x" coordinate: a function that takes points as input and outputs real numbers.



$$x(P) = 3$$

When we say "the equation of a circle is $x^2+y^2=1$" what we mean is that if you test every point P in the plane, by measuring its x-coordinate $x(P)$, its y-coordinate $y(P)$, and then compare $x(P)^2+y(P)^2$ to 1, the set of points that "pass" is (by definition) the circle of radius 1. We write

$$\begin{aligned} S^1 &= \{ P \mid x(P)^2+y(P)^2 = 1 \} \\ &= \{ P \mid x(P)^2+y(P)^2-1 = 0 \} \end{aligned} \tag{2.1}$$

So what kind of thing is x^2+y^2-1? We could say: it is a function, that on input P returns $x(P)^2+y(P)^2-1$. And this is true, but the expression x^2+y^2-1 does more than specify the set of input/output pairs $(P, x(P)^2+y(P)^2-1)$, it specifies a rule or algorithm for computing the output. The expression $x(P)^2+y(P)^2-1+2-2$ gives another rule for computing the same function (of course there are less trivial examples). Although we often conflate "function" with "rule", strictly speaking a function is just the input output pairs

$$\ulcorner \text{A function } F: X \longrightarrow Y \text{ is the set } \{(x, F(x)) \mid x \in X\} \lrcorner \tag{2.2}$$

Polynomials

Fine, so what is x^2+y^2-1? It is a polynomial, which is a special kind of rule for computing numbers (not a function, although any polynomial determines a function). To explain what a polynomial is, we consider some examples

$$2x^2+3x-2$$

x^0	x^1	x^2	x^3	x^4	
0	1	2	3	4	...
-2	3	2	0	0	...

why not y^2x?

(2.3)

$$3x^2y+y^2+2x^2+1$$

x^0y^0	x^2y	x^2	y^2	
(0,0)	(2,1)	(2,0)	(0,2)	...
1	3	2	1	...

We will refer to <u>fields</u>, for which you may read $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Recall $\mathbb{N} = \{0,1,2,\ldots\}$.
Let k be a field. A <u>polynomial f in n variables with coefficients in k</u> is an assignment of "coefficients" $\mathrm{coeff}(f,\alpha) \in k$ to tuples $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$, with only finitely many tuples being assigned nonzero values.

A polynomial which assigns 1 to exactly one α and 0 to the rest is called a <u>monomial</u>, and we denote it by x^α (for some formal symbol α). Addition and multiplication of polynomials is defined by

$$\mathrm{coeff}(f+g,\alpha) = \mathrm{coeff}(f,\alpha) + \mathrm{coeff}(g,\alpha)$$

$$\mathrm{coeff}(fg,\alpha) = \sum_{\substack{\gamma+\beta=\alpha \\ \gamma,\beta\in\mathbb{N}^n}} \mathrm{coeff}(f,\beta)\,\mathrm{coeff}(g,\gamma) \tag{3.1}$$

$$\lambda \in k \qquad \mathrm{coeff}(\lambda f,\alpha) = \lambda\,\mathrm{coeff}(f,\alpha)$$

Two polynomials f,g are equal, written $f=g$, if they have the same coefficients, $\mathrm{coeff}(f,\alpha) = \mathrm{coeff}(g,\alpha)$ for all α. Given variable names, e.g. $x_1,\ldots,x_n$, we define the polynomials x_i to be the monomials x^{e_i} where $e_i = (0,\ldots,\overset{i}{1},\ldots,0)$. We write $1 = x^{\underline{0}}$ for the polynomial with $\mathrm{coeff}(1,\underline{0}) = 1$, and if $\lambda \in k$ we also write λ for the polynomial $\lambda 1$, i.e. $\mathrm{coeff}(\lambda 1, \underline{0}) = \lambda$.

<u>Exercise 1.1</u> (i) $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ where for $m \in \mathbb{N}$, and a polynomial f, we write f^m for $\underbrace{f\cdots f}_{m}$.

(ii) $x^\alpha x^\beta = x^{\alpha+\beta}$ where addition on $\mathbb{N}^n$ is coordinate-wise.

(iii) If $\alpha^{(1)},\ldots,\alpha^{(m)}$ are distinct elements of $\mathbb{N}^n$ then $f = a_1 x^{\alpha^{(1)}} + \cdots + a_m x^{\alpha^{(m)}}$ is the polynomial with $\mathrm{coeff}(f,\alpha^{(i)}) = a_i$ for $1 \le i \le m$.

<u>Def^n</u> The set of polynomials in n-variables is P_n, or if we want to fix names for the variables, $k[x_1,\dots,x_n]$.

The set of polynomials $k[x_1,\dots,x_n]$ is a <u>commutative ring</u>, which just means that you can add and multiply polynomials in a way that satisfies the usual algebraic properties for integers. We will not dwell on these properties here, but simply highlight that multiplication distributes over addition $f(g+h) = fg + fh$.

<u>Def^n</u> Given $f, g \in k[x_1,\dots,x_n]$ we say <u>f divides g</u> (written $f \mid g$) if there exists $h \in k[x_1,\dots,x_n]$ with $g = fh$

<u>Example 1.1</u> (i) $x^2+y^2-1 \in k[x,y]$

(ii) $2x^2+3x-2 \in k[x]$

(iii) $3x^2y + y^2 + 2x^2 + 1 \in k[x,y]$

(iv) $2x + 3x = 5x \in k[x]$

(v) $1 + x + x^2 + x^3 + \cdots \notin k[x]$

<u>Lemma 1.1</u> If $f \in k[x_1,\dots,x_n]$ and $\Lambda = \{\alpha \in \mathbb{N}^n \mid \mathrm{coeff}(f,\alpha) \neq 0\}$ then $f = \sum_{\alpha\in\Lambda} a_\alpha x^\alpha$ where $a_\alpha = \mathrm{coeff}(f,\alpha)$.

<u>Proof</u> By def^N

$$\begin{aligned}\mathrm{coeff}\left(\textstyle\sum_\alpha a_\alpha x^\alpha, \beta\right) &= \textstyle\sum_\alpha \mathrm{coeff}(a_\alpha x^\alpha, \beta)\\ &= \textstyle\sum_\alpha a_\alpha \,\mathrm{coeff}(x^\alpha,\beta)\\ &= \textstyle\sum_\alpha a_\alpha \,\delta_{\alpha=\beta} \quad \leftarrow \text{Kronecker delta, } 1 \text{ if } \alpha=\beta \text{ and } 0 \text{ otherwise}\\ &= a_\beta\end{aligned}$$

so the LHS and RHS have the same coefficients. $\square$

Generally we write polynomials f as $\sum_\alpha a_\alpha x^\alpha$ where it is understood the α are all distinct and there are only finitely many of them.

If $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ we write $|\alpha| = \alpha_1 + \dots + \alpha_n$.

Def^n Let $f \in k[x_1, \dots, x_n]$. Then with $f = \sum_\alpha a_\alpha x^\alpha$

- If $a_\alpha \neq 0$ we call $a_\alpha x^\alpha$ a term of f.
- If $f \neq 0$ the total degree of f is $\max\{ |\alpha| \mid a_\alpha \neq 0 \}$.

Example 1.2 $3x^2y + y^2 + 2x^2 + 1$ has four terms and total degree 3.

Now we know to think of polynomials as finite data structures assigning coefficients a_α to tuples $\alpha \in \mathbb{N}^n$. There is an associated polynomial function:

Def^n Given $f \in k[x_1, \dots, x_n]$ define $F : k^n \longrightarrow k$ by, if $f = \sum_\alpha a_\alpha x^\alpha$,

$$F(\lambda_1, \dots, \lambda_n) = \sum_\alpha a_\alpha \underbrace{\lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}}_{\text{ops in } k}$$

As a set, F is $\{ (\underline{c}, F(\underline{c})) \mid \underline{c} \in k^n \}$ which is infinite if k is. We will often elide the distinction between f and F and just write f for both. This seems like it might be confusing, because if g is another polynomial with function G then

- $f = g$ means equality as polynomials (i.e. $\mathrm{coeff}(f, \alpha) = \mathrm{coeff}(g, \alpha)$ for all α)

- $F = G$ means equality as functions (i.e. $F(\underline{c}) = G(\underline{c})$ for all $\underline{c} \in k^n$)

Clearly $f = g$ implies $F = G$. The converse is also true:

P iff Q means $P \Rightarrow Q$ and $Q \Rightarrow P$
"converse"

<u>Proposition</u> CLO 1.1.5 Let k be an infinite field and $f \in k[x_1, \dots, x_n]$ with function $F : k^n \to k$. Then $f = 0$ if and only if $F = 0$.

<u>Proof</u> We prove the converse by induction on n. If $n = 1$ then a nonzero polynomial of degree m has at most m roots (we will reprove this later). Suppose $F = 0$ but that $f \neq 0$. Then f has degree m say, and hence at most m roots, but $F = 0$ so f has $> m$ roots (since k has $> m$ distinct elements), a contradiction.

For the inductive step suppose the converse holds for $n \leq N$ and let $f \in [x_1, \dots, x_{N+1}]$. Suppose that $F = 0$. We can collect terms to write, for some $m \geq 0$,

$$f = \sum_{i=0}^{m} g_i(x_1, \dots, x_N)\, x_{N+1}^{i},$$

where $g_i \in k[x_1, \dots, x_N]$. For $\underline{c} = (c_1, \dots, c_N) \in k^N$ we have the polynomial

$$h_{\underline{c}} := f(c_1, \dots, c_N, x_{N+1}) = \sum_{i=0}^{m} \underbrace{g_i(c_1, \dots, c_N)}_{\text{in } k} x_{N+1}^{i} \in k[x_{N+1}]$$

Since $F = 0$, the function $H_{\underline{c}}$ associated to $h_{\underline{c}}$ is zero, $H_{\underline{c}} = 0$. But by the base case then we have $h_{\underline{c}} = 0$ as a polynomial, so $g_i(\underline{c}) = 0$ for $0 \leq i \leq m$. Since $\underline{c}$ was arbitrary this shows the functions G_i associated to g_i are zero, and by the inductive hypothesis $g_i = 0$ hence $f = 0$. $\square$

<u>Corollary</u> CLO 1.1.6 Let k be an infinite field, $f, g \in k[x_1, \dots, x_n]$ with functions F, G. Then $f = g$ if and only if $F = G$.

<u>Proof</u> Apply the Proposition to $f - g$. $\square$

Affine varieties

We have said algebraic geometry is the study of curves, surfaces and higher-dimensional objects defined by solutions of systems of polynomial equations. These are called <u>varieties</u>. Given a field k we write $\mathbb{A}^n_k$ or just $\mathbb{A}^n$ for <u>n-dimensional affine space</u>

$$\mathbb{A}^n = k^n = \{(a_1, \ldots, a_n) \mid a_i \in k \quad 1 \le i \le n\}.$$

The purpose of the notation is to emphasise k^n as an object of algebraic geometry, as opposed to a vector space, for example.

<u>Def^n</u> Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then we define

$$\mathbb{V}(f_1, \ldots, f_s) = \{ \underline{a} \in \mathbb{A}^n \mid f_i(\underline{a}) = 0 \text{ for } 1 \le i \le s \}$$

and call this the <u>affine variety</u> determined by $f_1, \ldots, f_s$. This depends only on the set $\{f_1, \ldots, f_s\}$, so order does not matter.

For the moment we only allow <u>finite</u> systems of equations $f_1, \ldots, f_s$. But watch this space!

<u>Remark</u> If $f = 0$ then $\mathbb{V}(f) = \mathbb{A}^n$, so $\mathbb{A}^n$ is an affine variety.
If $f = 1$ then since $0 \neq 1$ (careful now!) $\mathbb{V}(f) = \phi$, the empty set.

<u>Lemma CLO 1.2.2</u> If $V, W \subseteq \mathbb{A}^n$ are affine varieties, so are $V \cup W$ and $V \cap W$.

<u>Proof</u> If $V = \mathbb{V}(f_1, \ldots, f_s)$, $W = \mathbb{V}(g_1, \ldots, g_t)$ then $V \cap W = \mathbb{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$, so one claim is clear. For the other, we claim

$$V \cup W = \mathbb{V}(\{f_i g_j\}_{1 \le i \le s, 1 \le j \le t}).$$

The inclusion $\subseteq$ is clear. For the reverse inclusion, suppose

$$\underline{a} \in \mathbb{V}(\{f_i g_j\}_{i,j})$$

If $\underline{a} \in W$ then we're done. Otherwise for $1 \le i \le s$

$$f_i(\underline{a}) g_1(\underline{a}) = \cdots = f_i(\underline{a}) g_t(\underline{a}) = 0.$$

If $f_i(\underline{a}) \neq 0$ then we deduce $\underline{a} \in W$, a contradiction, so $f_i(\underline{a}) = 0$. Since this holds for arbitrary i, we have $\underline{a} \in V$. $\square$

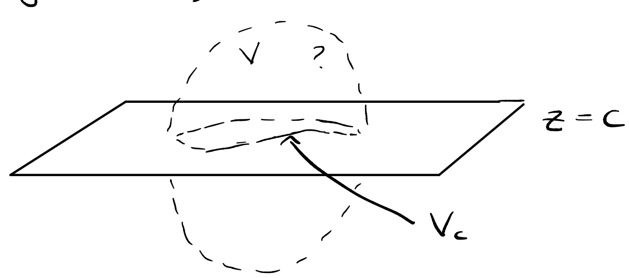
Hence finite unions and intersections of affine varieties are affine varieties. In the remainder of this lecture we study examples.

<u>Examples</u>

Consider the surface $V = \mathbb{V}(x^2 - y^2 z^2 + z^3)$. Given a polynomial $f = x^2 - y^2 z^2 + z^3$ in multiple variables it is not at all clear how to "sketch" $V = \mathbb{V}(f)$. Let us try some simple things, like intersecting V with a plane. This itself is a bit interesting, since a plane is an *affine variety*! For $c \in \mathbb{R}$ set

$$H_c = \{(a,b,c) \mid a,b \in \mathbb{R}\} = \mathbb{V}(z - c)$$

Hence $V \cap H_c = \mathbb{V}(x^2 - y^2 z^2 + z^3,\ z - c)$, which you should be able to see is $V_c = \mathbb{V}(x^2 - y^2 c^2 + c^3)$.



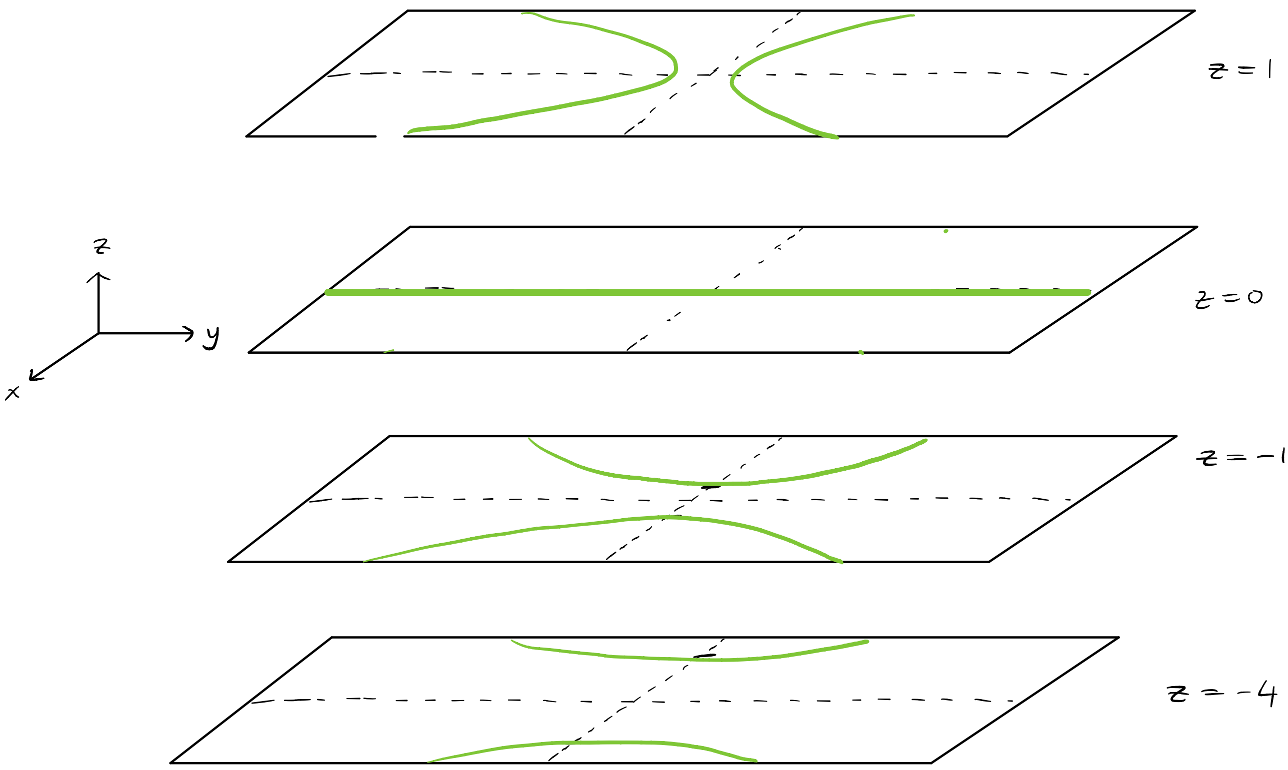
What do these "slices" V_c look like? If $c<0$ then

$$x^2 - y^2c^2 + c^3 = 0$$
$$\iff x^2 - (|c|y)^2 = |c|^3$$

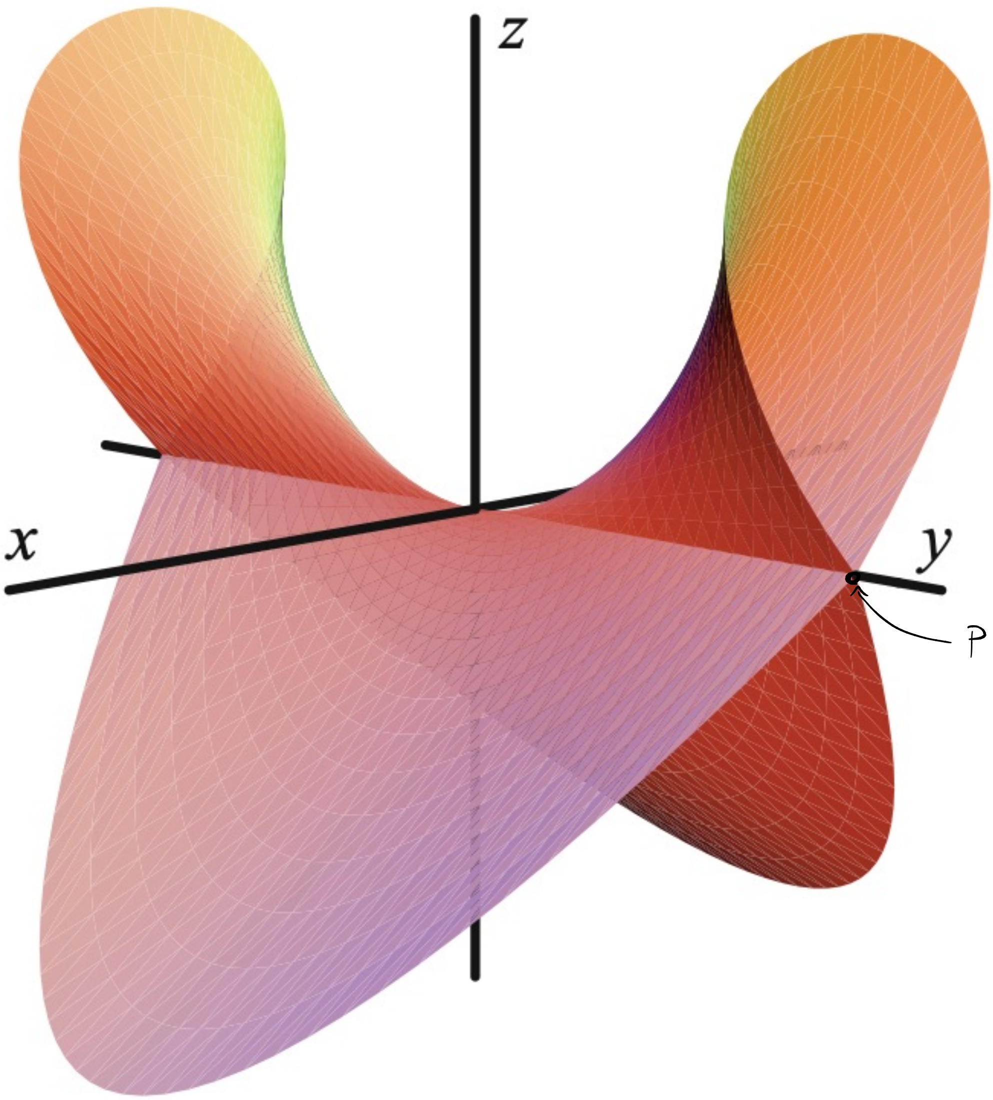
Is a hyperbola meeting the x-axis at $\pm |c|^{3/2}$. When $c=0$ we have $x^2=0$, so just the y-axis, and for $c>0$ we have

$$x^2 - y^2c^2 + c^3 = 0$$
$$\iff (cy)^2 - x^2 = c^3$$

another family of hyperbolas meeting the y-axis at $\pm c^{1/2}$.



The graph from CLO is:



We see how the surface intersects itself along the y-axis: near the point P, V does not locally look like an open ball in $\mathbb{R}^2$, but more like an "X" shape with a cartesian product with $(0,1)$. This explains why V is a natural object of <u>algebraic</u> geometry and not <u>differential</u> geometry. We say V is <u>singular</u>.

You might wonder how this plot was generated. In fact V has a convenient <u>parametrisation</u> by parameters u, v in the following sense:

Let $\varphi : [-1,1]^2 \longrightarrow \mathbb{R}^3$ be the function

$$\varphi(u,t) = \left(t(u^2-t^2),\ u,\ u^2-t^2 \right)$$

and set $Z := \operatorname{Im}\varphi = \{ \varphi(u,t) \mid u,t \in [-1,1]^2 \}$, the image of φ. Then $Z \subseteq V$ since if $x = t(u^2-t^2)$, $y = u$, $z = u^2-t^2$ then

$$\begin{aligned} x^2 - y^2z^2 + z^3 &= t^2(u^2-t^2)^2 - u^2(u^2-t^2)^2 + (u^2-t^2)^3 \\ &= (t^2-u^2)(u^2-t^2)^2 + (u^2-t^2)^3 \\ &= (t^2-u^2)^3 - (t^2-u^2)^3 = 0. \end{aligned}$$

One can show $Z = V$ (see Ex CLO 1.3.11), and we call φ a <u>parametrisation</u> of V. Note how this parametrisation "slices" along the y-axis instead. What kind of curves do we get in the xz plane when we do this?

Note how

- V is much easier to visualise when we have a parametrisation, <u>but</u>
- checking if $P \in V$ is much easier using the "implicit" form of the surface given by $x^2 - y^2z^2 + z^3 = 0$.

This leads to two questions which will be among the motivations for this course:

<u>Parametrisation</u> Does a given affine variety admit a parametrisation? (In general, <u>no</u>)

<u>Implicitisation</u> Given a parametric representation of an affine variety, can we determine a set of defining equations? Yes! we'll prove it.