Q1 K algebraically closed

$F(X,Y,Z)$ is homogeneous, nonconstant, coeffs in K.

Show $V(F) = \{[a,b,c] \mid F(a,b,c)=0\}$ is infinite.

Basic idea: Dehomogenise F to get $F_d(x,y)$. This will be nonconstant unless F is just a power of Z times constant.

$\left(\text{If } F = kZ^d \text{ then } F(a,b,0) = 0 \ \forall a,b \ \therefore V(F) \text{ infinite.} \right)$

So assume $F_d(x,y)$ is nonconstant, call it $f(x,y)$. Then $f(x,y)=0 \iff F(x,y,1)=0$

So it's enough to show that

$\{(x,y) \mid f(x,y)=0\}$ is infinite

- If $f(x,y)$ doesn't contain any x's, then it is a polynomial in 1 variable y which is nonconstant, say $\tilde{f}(y)$

$\therefore$ Since K is alg. closed, $\tilde{f}$ has a root y_0 say.

So $f(x,y_0) = \tilde{f}(y_0) = 0$

$\forall\, x$ $\therefore$ $\{(x,y) \mid f(x,y)=0\}$ is infinite

Similarly if $f(x,y)$ doesn't contain any y's.

- So assume $f(x,y)$ contains both x's and y's.

For any y_0 the polynomial

$f(x,y_0)$ has at least 1 root

unless it is constant.

So $\{(x,y) \mid f(x,y)=0\}$ is infinite

as long as there are only finitely many y_0's s.t. $f(x,y_0)$ is constant.

Remains to show:

only finitely many y_0 s.t. $f(x,y_0)$ is constant

To do this: write

$$f(x,y) = f_0(y) + f_1(y)x + \cdots + f_k(y)x^k$$

$f(x,y)$ does have x's in it

$\therefore$ at least one of $f_i(y)$ is nonzero

Then $f(x,y_0)$ is constant

$\iff$ y_0 is a common root of

$$f_1(y), f_2(y), \ldots, f_k(y)$$

Only finitely many such roots. $\square$.

2. p prime. Show

$$X^3 + pY^3 + p^2 Z^3 = 0 \quad (*)$$

has no solutions in $\mathbb{Q}^3 \setminus \{(0,0,0)\}$.

In other words if $F = X^3 + pY^3 + p^2 Z^3$

then ... in $\mathbb{P}^2_{\mathbb{Q}}$ the subset

$$V(F) = \{[a,b,c] \mid F(a,b,c) = 0\}$$

is <u>empty</u>.

<u>Solution:</u> suppose (q,r,s) is a solution of $(*)$

different from $(0,0,0)$

Since $(*)$ is homogeneous, ...

for any $a \in \mathbb{Q}$ we have that

(aq, ar, as) is also a solution.

By choosing a appropriately we can assume we have a solution where

$q, r, s \in \mathbb{Z}$ <u>and</u> $\gcd(q, r, s) = 1$.

Rewrite our equation as

$$X^3 = -p(Y^3 + pZ^3)$$

Substitute our solution:

$$q^3 = -p(r^3 + ps^3) \quad (*)$$

So $p \mid q^3 \therefore p \mid q$ (~~$p^3 \mid q^3$~~)

So we can write $q = pq'$ for some integer q'

So $(*)$ becomes

$$p^3 (q')^3 = -p(r^3 + ps^3).$$

$$\therefore \quad p^2 (q')^3 = r^3 + ps^3$$

i.e. $$r^3 + ps^3 + p^2 (q')^3 = 0.$$

i.e. $$r^3 = -p(s^3 + p^2 (q')^3).$$

So (r, s, q') is a new solution of our original equation.

Repeat the argument $\therefore$ get

$$r = pr' \quad \text{for some } r' \in \mathbb{Z}.$$

Repeat again: get

$$s = ps' \quad \text{for some } s' \in \mathbb{Z}.$$

So $p \mid q$, $p \mid r$, $p \mid s$

contradicting our assumption that

$$\gcd(q, r, s) = 1.$$

$\therefore$ No solution exists.

(This method is called "infinite descent".)

7. $$Y^2Z = X^3 - 2X^2Z + XZ^2$$

Show this is not an elliptic curve.

__Solution:__ Need to show $g(X,Z)$ is such that $g_d(x)$ does not have 3 distinct roots.

Here $g(X,Z) = X^3 - 2X^2Z + XZ^2$

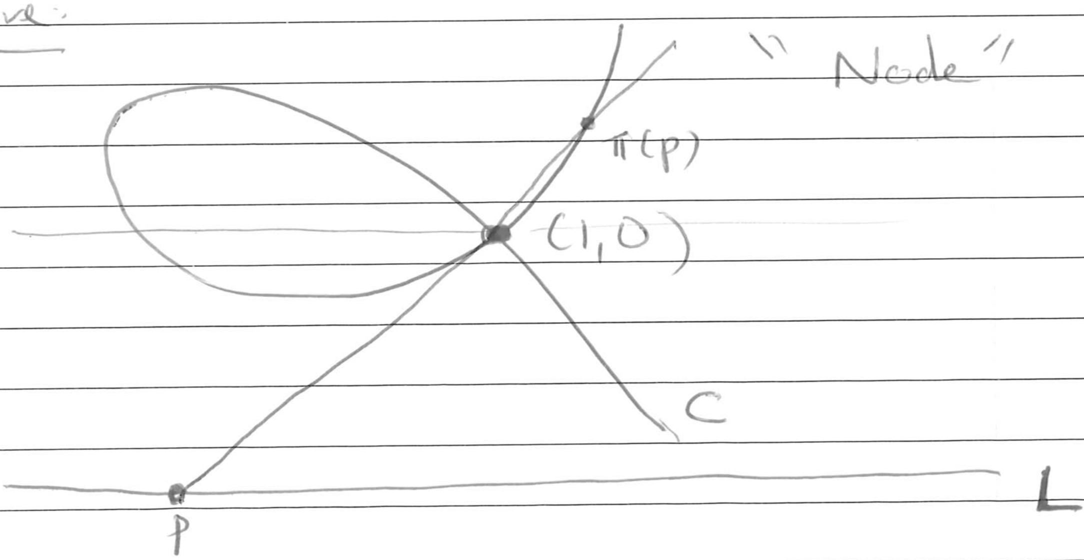
$$\therefore \quad g_d(x) = x^3 - 2x^2 + x$$

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

$$= x(x-1)^2$$

$\therefore$ only 2 distinct roots.

__Picture:__



The map $p \mapsto \pi(p)$ gives a "rational parametrisation" of the curve C.