Last time

for alg curve

$$E : y^2 = x^3 + Ax + B$$

$$\Delta(E) := 4A^3 + 27B^2 \neq 0$$

iff E has a tangent line at every point.

In the proof over an arbitrary $P = (x_0, y_0)$

last case: $m = \dfrac{3x_0^2 + A}{2y_0}$

if $2y_0 = 0 \wedge 3x_0^2 + A = 0$

$(\Rightarrow A < 0)$

$\Rightarrow A = -A$

$3x_0^2 - A = 0$

$(\Leftrightarrow) \quad 3x_0^2 = A$

not kosher

$\Rightarrow \quad x_0 = \pm\sqrt{\frac{A}{3}}$

$\vdots \quad \Leftrightarrow \quad \Delta(E) = 0$

instead: $x_0^2 = \frac{A}{3} \quad (\Delta)$

We have

$$x_0^3 - A x_0 + B = 0$$

$$\Rightarrow \quad x_0 \cdot \frac{A}{3} - A x_0 + B = 0$$

$$(\Rightarrow) \quad x_0 = -\frac{2}{3} \cdot \frac{B}{A} \quad (\star)$$

$$\Rightarrow \quad \frac{A}{3} = \frac{9B^2}{\quad}$$

$$4A^3 \qquad 4A^2$$

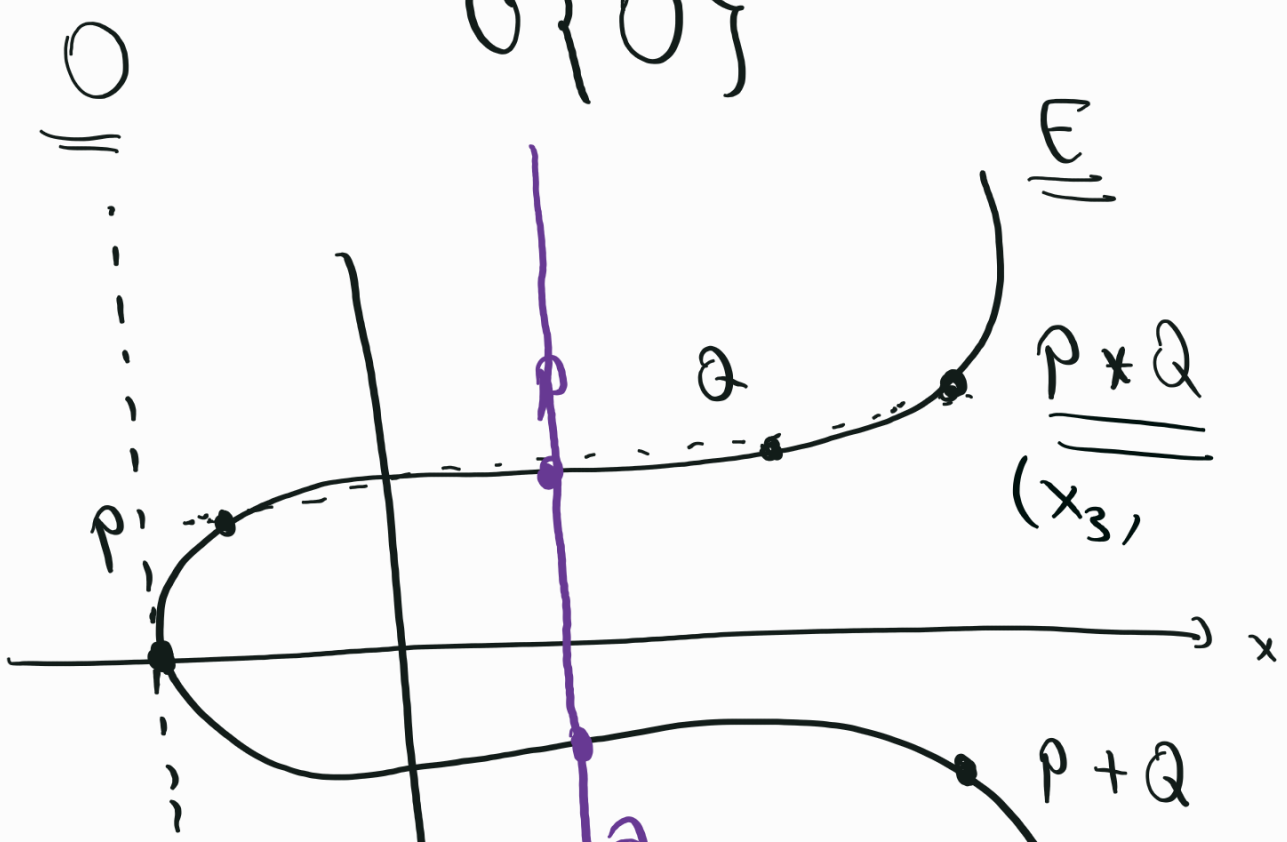
$$\Longleftrightarrow \quad 4A^3 - 27B^2 = 0$$

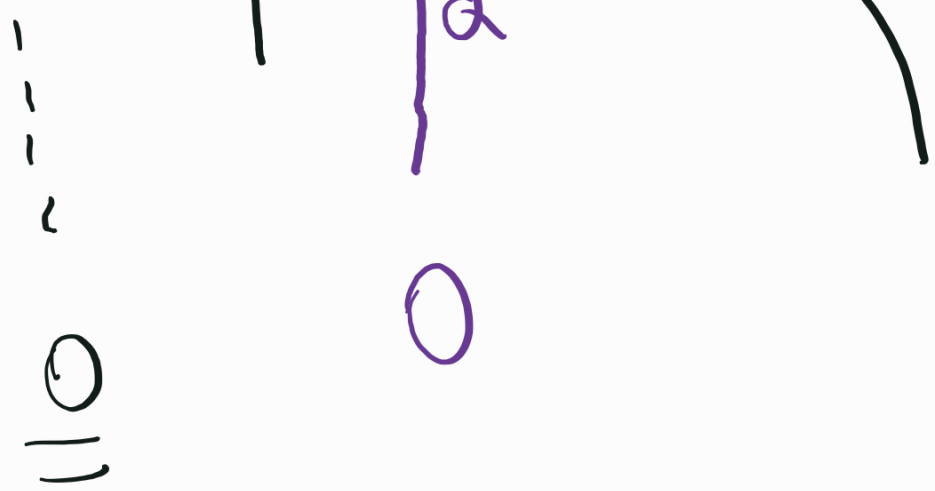
$$A := -A \quad (=) \quad 4A^3 + 27B^2 = 0$$

$E/\mathbb{k}$ an e.c.

$\mathbb{k}$-rational pts

$$E(\mathbb{k}) = \left\{ (x,y) \in \mathbb{k}^2 \;\middle|\; y^2 = x^3 + Ax + B \right\} \cup \{O\}$$





$\underline{\underline{0}}$

Construction of "+" over $\mathbb{K}$.

start w/ $P = (x_1, y_1)$

$Q = (x_2, y_2)$

and let L is the line that passes through P & Q.

so L $\underline{\underline{y = m(x - x_1) + y_1}}$

where $m = \underline{\underline{\dfrac{y_2 - y_1}{x_2 - x_1}}}$

If $x_1 = x_2$ L is

Vertical ... later.

Suppose $x_1 \neq x_2$.

$$L: \quad y = m(x - x_1) + y_1$$

$L \cap E$

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

$\Leftrightarrow$

$\vdots$

$$\rightarrow (*) \quad 0 = x^3 - m^2 x^2 + \cdots$$

We know that x_1, x_2 are roots of $(*)$ and also, over $\overline{k}$:

$\searrow$

$$(**) \quad (x - x_1)(x - x_2)(x - x_3) = 0$$

$\Leftrightarrow$

(***) $0 = x^3 - (x_1 + x_2 + x_3)x^2 + \cdots$

$\Rightarrow x_1 + x_2 + x_3 = m^2 \in \mathbb{k}$

$\Rightarrow x_3 \in \mathbb{k}$

$\Rightarrow y_3 = -(m(x - x_1) + y_1)$

$\Rightarrow P + Q = (x_3, y_3).$

$(P \neq Q, \; x_1 \neq x_2, \; P, Q \neq 0)$

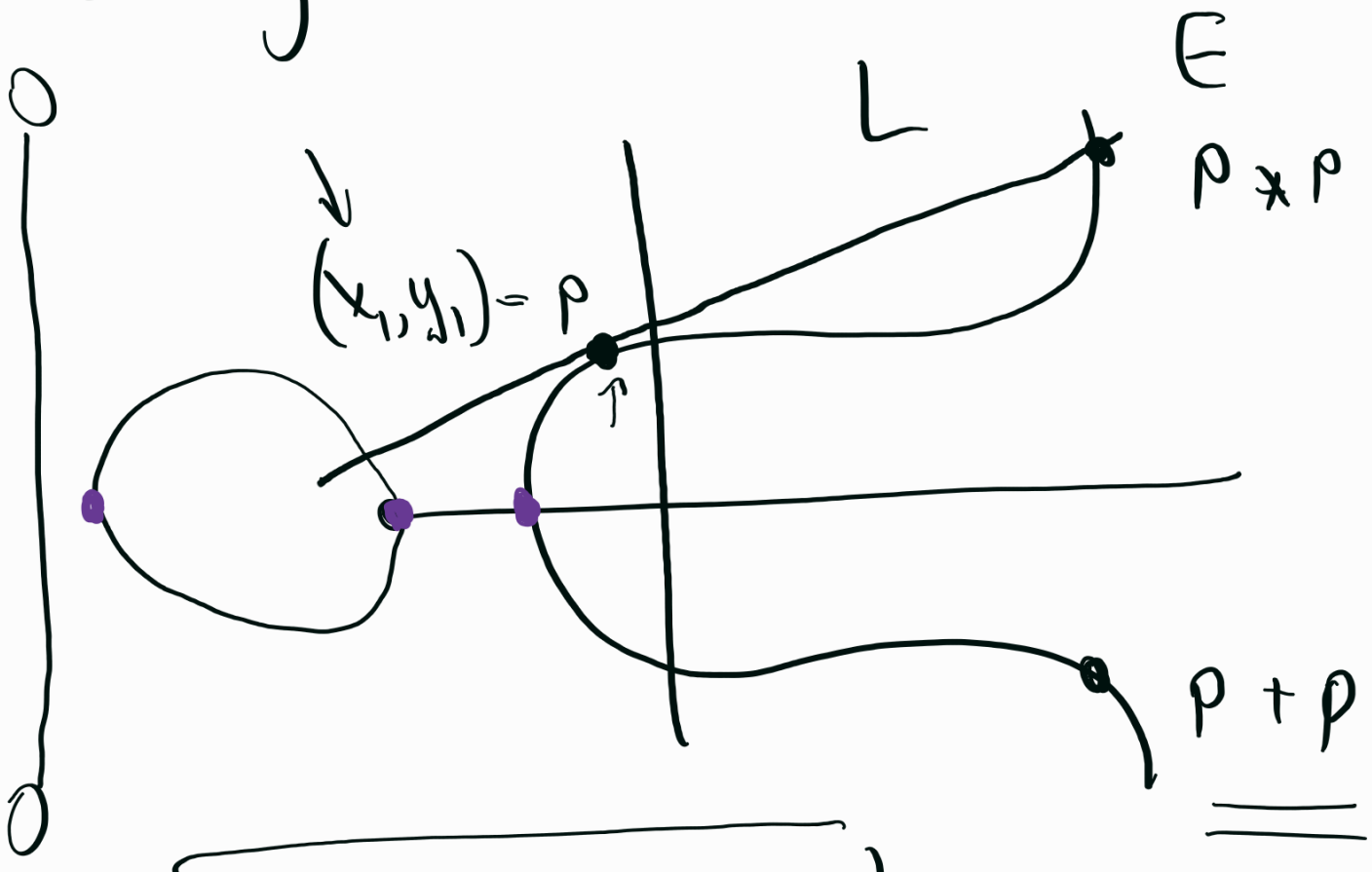
In case $x_1 = x_2$ but $y_1 \neq y_2$

Then L is vertical

then $P * Q = 0$

$\Rightarrow P + Q := 0.$

lastly if $P = Q$. (and $P, Q \neq O$)



$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

if $y_1 = 0$ then L is vertical $\Rightarrow P * P = O$

$\Rightarrow P + P = O$

o/w,

$$L: \quad y = m(x - x_1) + y_1$$

$$g(x) := x^3 + Ax + B - \left(m(x - x_1) + y_1\right)^2$$

clearly $g(x_1) = 0$

We claim that x_1 is a double root of g:

$$D(g)(x) = 3x^2 + A - 2m(mx + y_1 - mx_1)$$

derivative. $=$

$$D(g)(x_1) = \ldots = 0$$

$\overline{\mathbb{K}}$

$$\Rightarrow \quad g(x) = (x - x_1)^2 \cdot (x - x_3)$$

$$\Rightarrow \ldots \quad m^2 = x_1 + x_1 + x_3$$

$$\Rightarrow \quad x_3 = m^2 - 2x_1 \in \mathbb{K}$$

thus in this case

$$P+Q = \left(x_3, -m(x_3-x_1)-y_1\right)$$

Projective coordinates

Def: Let $\mathbb{k}$ be a field and

Consider $\mathbb{A}^3_{\mathbb{k}} := \mathbb{k} \times \mathbb{k} \times \mathbb{k}$.

Define $\sim$ on $\mathbb{A}^3 \setminus \{(0,0,0)\}$

by setting $(x,y,z) \sim \lambda(x,y,z)$

for any $\lambda \in \mathbb{k}^\times$

Exercise: $\sim$ is indeed

equivalence rel'n:

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$$

$$\wedge \; (x_2, y_2, z_2) \sim (x_3, y_3, z_3)$$

$$\Rightarrow (x_1, y_1, z_1) = \lambda_1 (x_2, y_2, z_2)$$

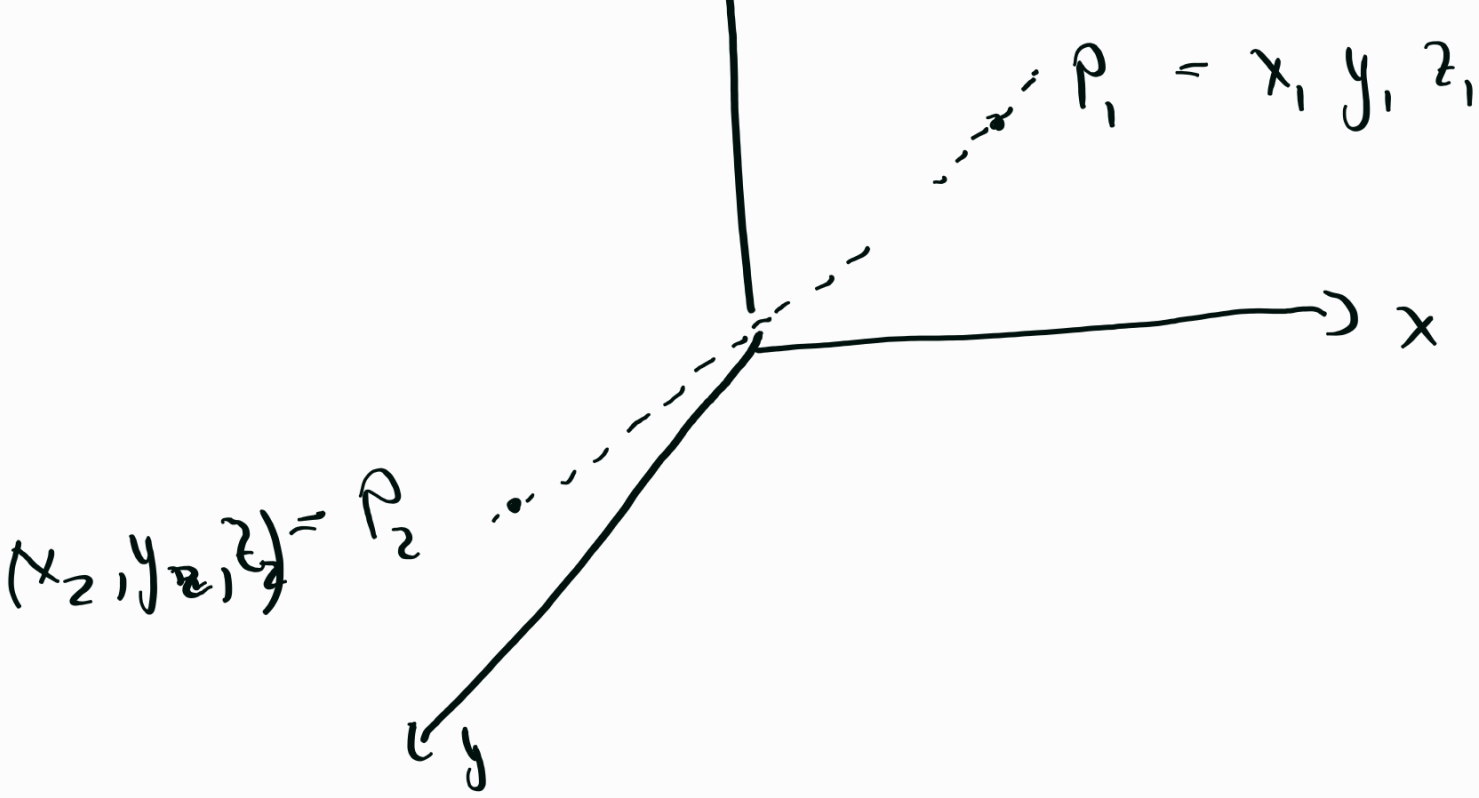
$$(x_2, y_2, z_2) = \lambda_2 (x_3, y_3, z_3)$$

$$\Rightarrow (x_1, y_1, z_1) = \lambda_1 \lambda_2 (x_3, y_3, z_3).$$

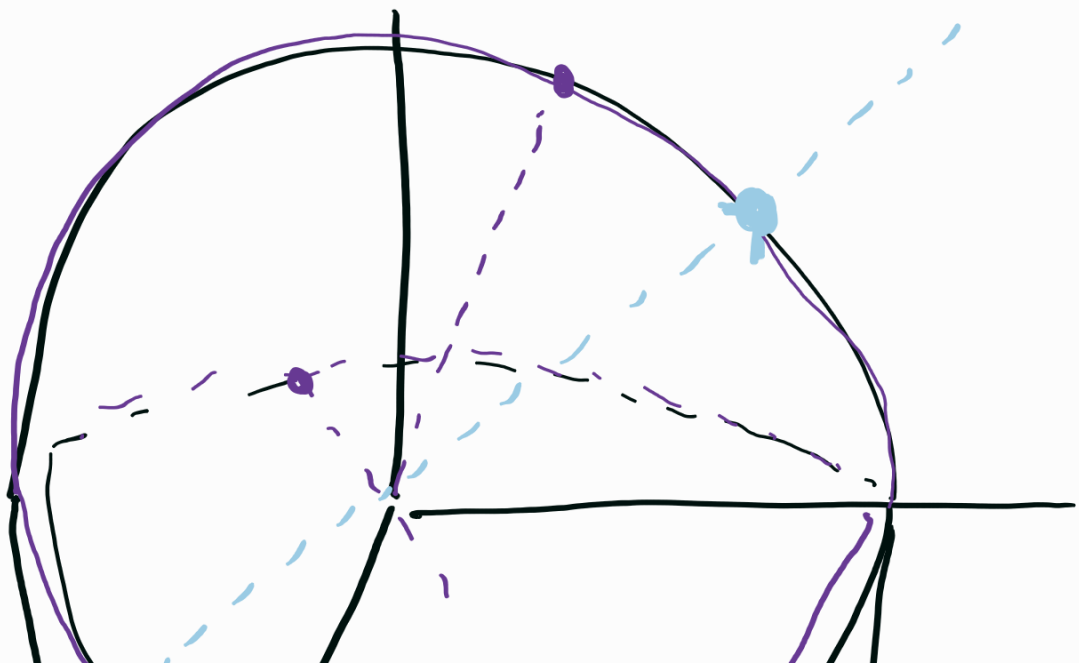
The projective plane is

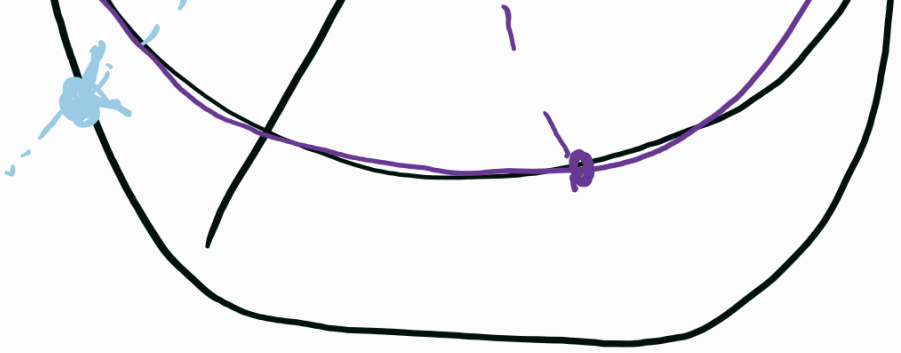
$$\mathbb{P}^2_{\mathbb{k}} := \mathbb{A}^3_{\mathbb{k}} \setminus \{(0,0,0)\} \Big/ \sim$$

Over $\mathbb{R}$:



We denote $(x : y : z)$ the equivalence class of (x, y, z) in $\mathbb{P}^2_{\mathbb{K}}$.





We call points $(x:y:0)$

points at infinity

and points w/ $z \neq 0$

$$(x:y:z) = \left(\frac{x}{z}:\frac{y}{z}:1\right)$$

affine points.

Def: A line in $\mathbb{P}^2_{\mathbb{k}}$ is

the solution set of

$$ax + by + cz = 0$$

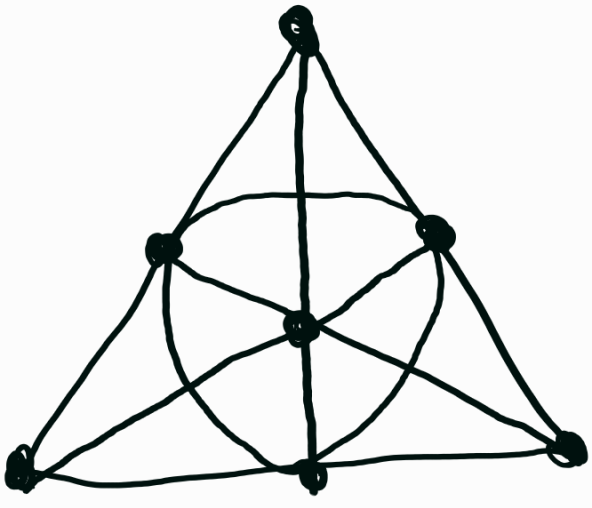
for some $a, b, c \in k$.

$$L : \{ (x:y:z) \mid ax+by+cz = 0 \}$$

Example Fano plane:

$$\# \mathbb{P}^2_{\mathbb{F}_2} = \# \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \setminus \{(0,0,0)\} / \sim$$

$$= \# \mathbb{F}_2^3 \setminus \{(0,0,0)\} = 7$$



Def.: A poly nomial f in 3

Def: A polynomial in x, y, z variables over k is a sum of monomials $a_{ijk} x^i y^j z^k$

where $a_{ijk} \in k$

$F(x,y,z)$ is called

homogeneous of degree n if all its monomials $a_{ijk} x^i y^j z^k$ satisfy $i+j+k=n$.

If $F(x,y,z)$ is homogeneous of degree n,

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x,y,z)$$

so $F(x,y,z) = 0 \iff$

$$F(\lambda x, \lambda y, \lambda z) = 0.$$

so $Sol(F)$ is well defined in $\mathbb{P}^2_k$.

- If $f(x,y) \in k[x,y]$, $\deg f = n$

then $F(x,y,z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$

is a homogeneous poly of degree n

Then $F(x,y,1) = f(x,y)$.

Example

$$f(x,y) = x^3 + Ax + B - y^2$$

$$F(x,y,z) = x^3 + Ax\cdot z^2 + Bz^3 - y^2\cdot z$$

$$F(x,y,1) = f(x,y)$$

Example: if $L: y = mx + a$

a line in $\mathbb{A}^2 = k \times k$

then $\tilde{L}: y = mx + az$

is a line in $\mathbb{P}^2_k$

the point of L can

be identified as the point on $\grave{L}$ which are affine ie $(x:y:1)$

suppose

$$L_1 : y = mx + b_1$$

$$L_2 : y = mx + b_2$$

parallel lines in $\mathbb{A}^2$

in $\mathbb{P}^2_k$:

$$\grave{L}_1 : y = mx + b_1 z$$

$$\grave{l} : y = mx + b_2 z$$

L_2 $\quad$ 0

- Points in $L_1 \cap L_2$

are solutions to

$$y - mx - b_1 z - (y - mx - b_2 z)$$

$$= (b_2 - b_1) z$$

and if $z = 0$ then

$$y = mx$$

so $(x : mx : 0)$

$$= (1 : m : 0)$$

We now look at in $\mathbb{A}^2_k$

$$C : \quad x^3 + Ax + B - y^2 = 0$$

$E: x^3 + Axz^2 + Bz^3 - y^2z = 0$

$E(k)$ (x,y)

in $\mathbb{P}^2_k$ $\longleftrightarrow$ $(x:y:1)$

$E': x^3 + Axz^2 + Bz^3 - y^2z = 0.$

$=$

What are the non-affine points of E' in $\mathbb{P}^2_k$?

set $z = 0$. $\Rightarrow x^3 = 0$

$\Rightarrow x = 0$

So $(0:y:0) \sim (0:1:0)$

is the only non

- affine point on E'.

E' is called a projective elliptic curve if $\Delta(E) \neq 0$.

$\Rightarrow$ $E/\mathbb{k}$ an e.c

$E(\mathbb{k})$ is an abelian gp

$F(x, y, z) = 0$

$\Leftrightarrow \quad F(\lambda x, \lambda y, \lambda z) = 0$

$\mathbb{P}^2_k \qquad (x,y,z) \sim \lambda(x,y,z)$

$\lambda^1 \quad \lambda^0$

$F(x,y,z) = x + 1 \cdot z$

$S_0 l(F) = \{(-1, x, y)\}$

$\mathbb{P}^2 \qquad (-1 : x : y) = (1 ; -x ; -y)$

$\in \quad S_0 l(F)$ $\qquad$ ~~$\in$~~ $S_0 l(F)$

$F(x,y,z) = 0$

$(*)$

$\hookrightarrow \quad F(\lambda x, \lambda y, \lambda z) = 0$

$$G(x, y, z) = x + z$$

Sol $(x + z)$

$$G(\lambda x, \lambda y, \lambda z)$$