$E(\mathbb{k}) = \{(x,y) \in \mathbb{k}^2 / y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$

Observe: (1) For $E/\mathbb{k}: y^2 = x^3 + Ax + B$, $A, B \in \mathbb{k}$

if $\mathbb{k} \subseteq \mathbb{L}$ is a field extension of $\mathbb{k}$ then

$$E(\mathbb{k}) \subseteq E(\mathbb{L})$$

is a subgp inclusion.

(2) Say $\mathbb{k} = \mathbb{F}_q$ for $q = p^n$, $n > 1$ prime power. $E/\mathbb{F}_q$, $A, B \in \mathbb{F}_q$, $\mathbb{F}_p$

$$\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q^2} \subseteq \mathbb{F}_{q^3} \subseteq \mathbb{F}_{q^6} \subseteq \cdots \subseteq \bar{\mathbb{F}}_q$$

$$\bar{\mathbb{F}}_q = \text{"} \cup \mathbb{F}_{q^n} \text{"}$$

$\Rightarrow$ a tower of subgp inclusions.

$$E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^2}) \subseteq \cdots \subseteq E(\overline{\mathbb{F}}_q)$$

(3) each $E(\mathbb{F}_{q^n})$ is a finite abelian gp

but

$E(\overline{\mathbb{F}}_q)$ is never finite!

Take $y_0 \in \overline{\mathbb{F}}_q$.

Then $\varphi(x) = x^3 + Ax + B - y_0^2$ is a poly over $\overline{\mathbb{F}}_q$

hence $\exists\ x_0 \in \bar{\mathbb{F}}_q$ s.t.h

$y_0 \neq y_0'$

$x_0 \quad \varphi(x_0) = 0 \quad \Rightarrow$

$\|$

$(x_0', y_0') \neq (x_0, y_0) \in E(\bar{\mathbb{F}}_q)$

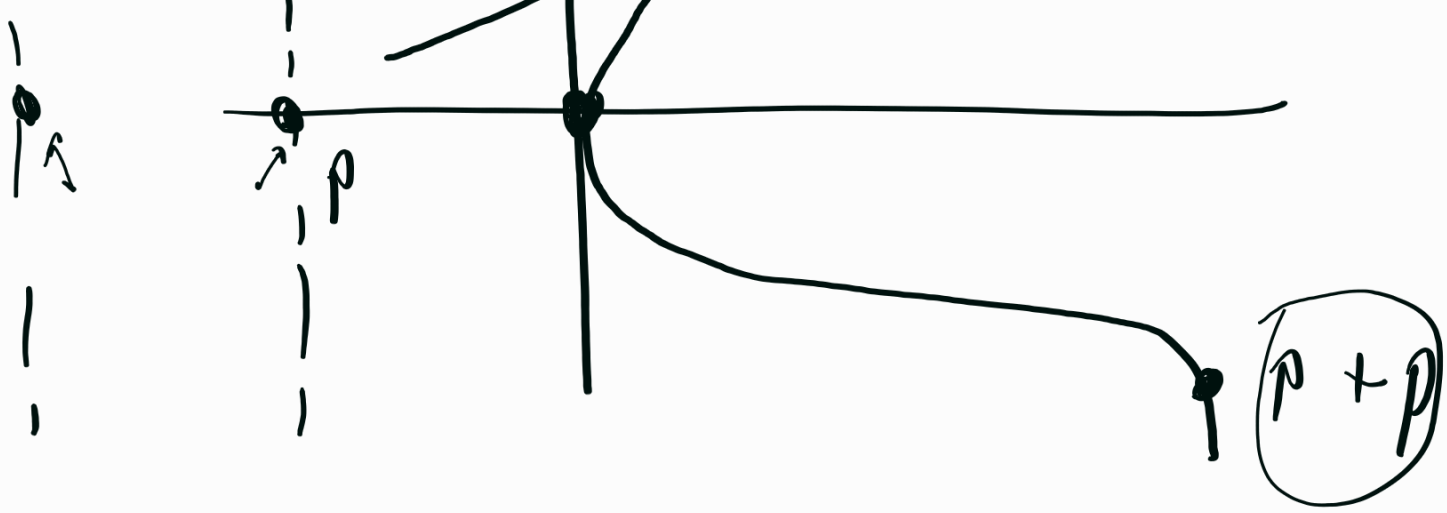
Since $\bar{\mathbb{F}}_q$ is infinite,

So is $E(\bar{\mathbb{F}}_q)$.

(4) What are the point of order 2 in $E(\bar{\mathbb{F}}_q)$?

ie $P \in E(\bar{\mathbb{F}}_q)$ s.t.h

$O \quad 2P = O$. $\Leftrightarrow$ the tangent to E at P is vertical



$O \quad P + P = O.$

So $\quad 2P = O$

$\Leftrightarrow \quad \boxed{P = (x_0, 0)}$

for $E/\bar{F}_q : \; y^2 = x^3 + Ax + B$

So x_0 is a root of

$s_E(x) = x^3 + Ax + B$

over $\bar{F}_q$.

Write

$$s_E(x) = (x - x_3)(x - x_1)(x - x_2)$$

and the

The points of order 2

$$E[2] = \{0\} \cup \{(x_0, 0), (x_1, 0), (x_2, 0)\}$$

in fact, $E[2] \leq E(\bar{\mathbb{F}}_q)$

and by the classification

of finite abelian gps

$$E[2] \cong \begin{cases} \mathbb{Z}_4 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{cases}$$

We will see that "klein gp"

$$E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$$

More generally

$$E[n] \subseteq E(\bar{\mathbb{F}}_q)$$

are the points of order n.

Last time $E/k : y^2 = x^3 + Ax + B$

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

$$k[E] = k[x,y]/(\varphi)$$

is $k[x]/(\quad)$ $f(x) \in k[x]$

$$/(\varphi(x)) \qquad r(x) \in k(x)$$

$$\times \quad f(x) = q \varphi(x) + r(x)$$

$$f(x) = r(x) \quad \text{in} \quad k[x]/(\varphi)$$

$$\Leftrightarrow \quad k[x] \times k[x] / \sim$$

$$f(x) \sim r(x)$$

$$\Leftrightarrow \quad \varphi \mid f - r$$

$$k[\epsilon] = k[x,y] \times k[x,y] / \sim$$

$$f(x,y) \sim r(x,y)$$

$$\Leftrightarrow \varphi \mid f - r$$

eg. $(x-y) \mid (x-y)(x+y)$

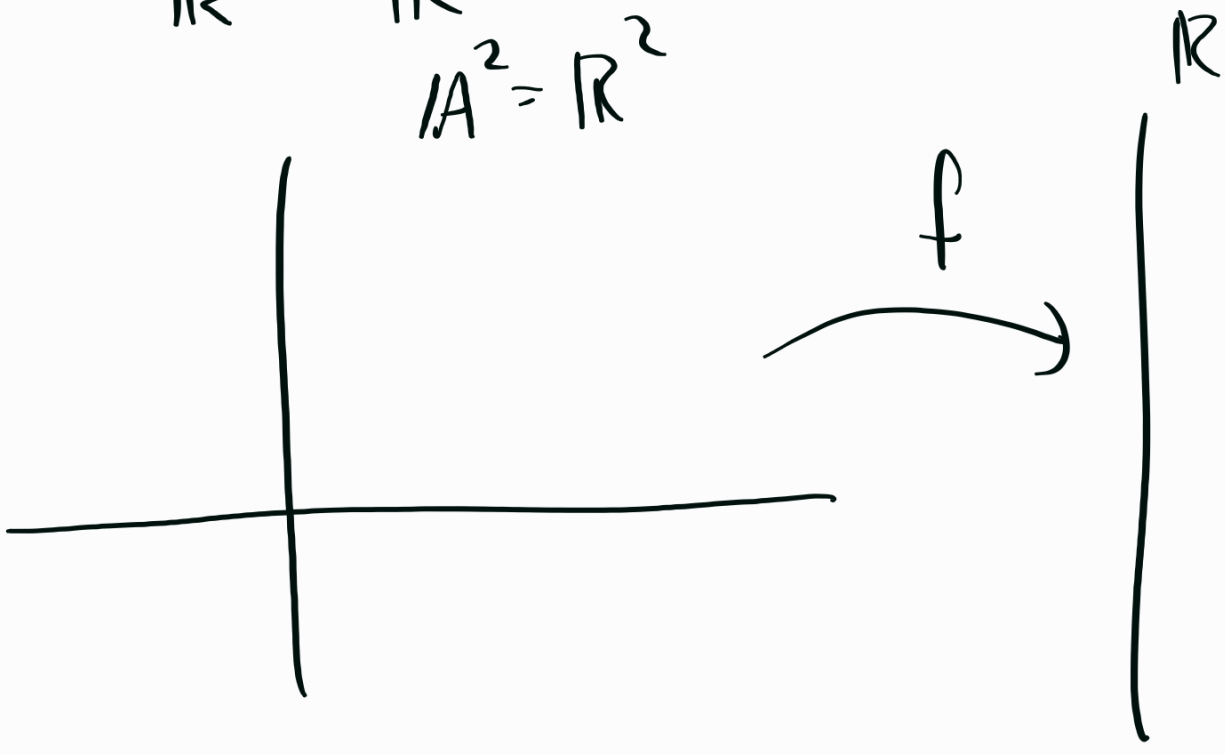
If $f \in \mathbb{k}[x,y]$

then

$$f : \mathbb{k}^2 \longrightarrow \mathbb{k}$$

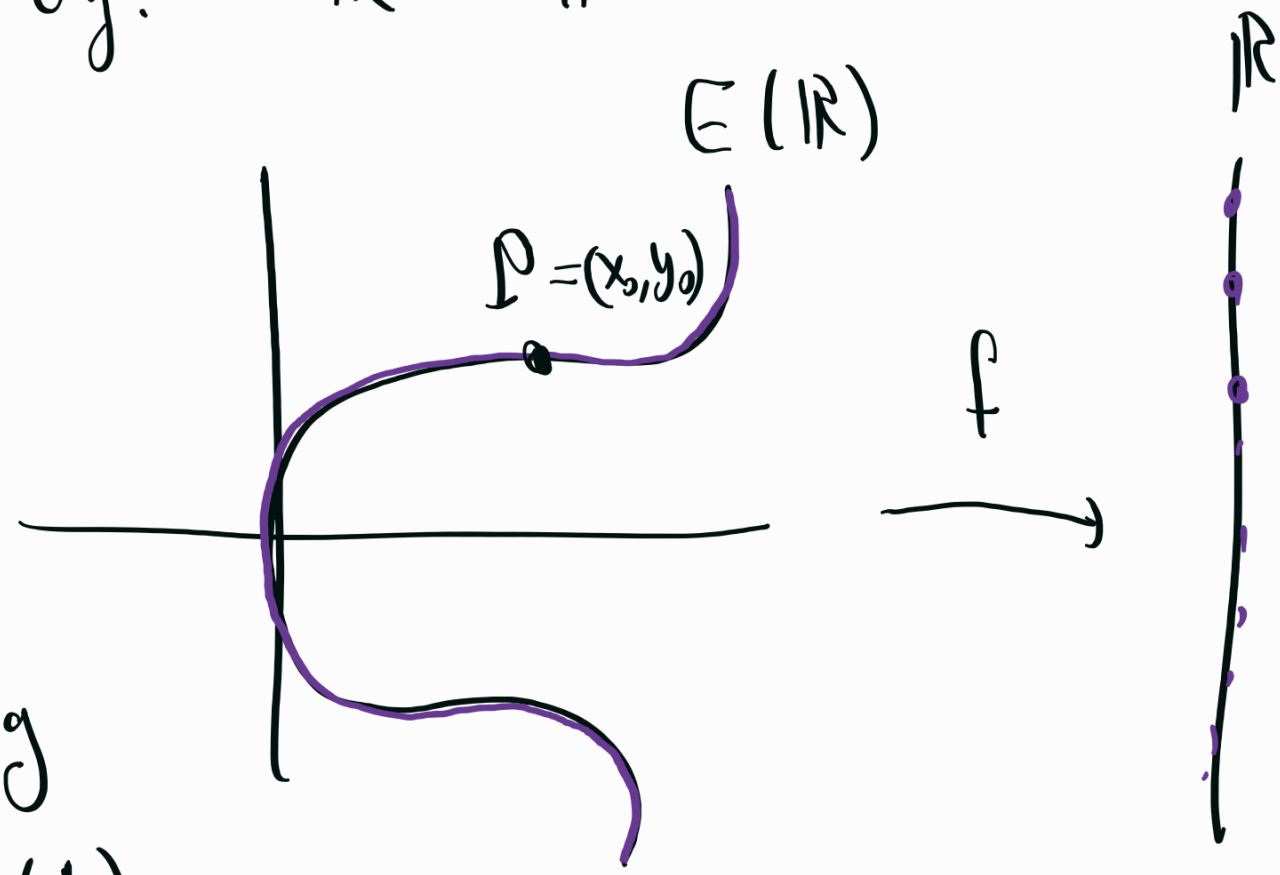
eg. $\mathbb{k} = \mathbb{R}$

$\mathbb{A}^2 = \mathbb{R}^2$



For $f \in \mathbb{k}[E]$

e.g. $\mathbb{k} = \mathbb{R}$ $\quad f(P)$



$f \sim g$

$P \in E(\mathbb{k})$

$\Rightarrow f(P) = g(P)$ in general

$$f \in \mathbb{k}[E]$$

$$f : E(\mathbb{k}) \setminus \{O\} \to \mathbb{k}$$

---

we defined

$$\mathbb{k}(E) = \mathbb{k}[E] \times \mathbb{k}[E] \setminus \{0\} /$$

$\Bbbk(E)$

$$\frac{f}{g} \sim \frac{f'}{g'}$$

$$(f, g) \sim (f', g')$$

$$\overset{\text{def}}{\iff} \quad f \cdot g' = f' g \quad \text{in } \Bbbk[E]$$

$$\left(\text{ie} \iff \varphi \mid f g' - f' g \right)$$

given $r \in \Bbbk(E)$

$$r : E(\Bbbk) \dashrightarrow \Bbbk = \mathbb{A}^1$$

(partial function)

r is <u>regular</u> at

$P \in E(\Bbbk)$ if $\exists$

a representation

a representation

$$r = \frac{f}{g} \in k(E)$$

s.th $g(P) \neq 0$.

then $r(P) = \dfrac{f(P)}{g(P)} \in k$

If r is not regular at P, $r(P) = \infty$

$\rightsquigarrow$

$$\underline{\underline{r}} : E(k) \setminus \{O\} \to \mathbb{P}^1$$

$$= k \cup \{\infty\}$$

$$\mathbb{P}^1 = k^2 \setminus \{(0,0)\} / \sim$$

$\mathbb{P}^1_{\mathbb{k}}$

$(x,y) \sim (\lambda x, \lambda y) \quad \forall_{\substack{\lambda \neq 0 \\ \in \mathbb{k}}}$

$[x : y]$

if $y \neq 0$ — Affine / finite ✓

$$[x:y] = \left[\frac{x}{y} : 1\right]$$

if $y = 0$ then

$$[x : 0] = [x' : 0]$$

↑ pt at infinity.

$$\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$$

$$x \longmapsto [x:1]$$

For $r \in \mathbb{k}(E)$ we want to define $r(0)$

In one variable

$$r(x) = \frac{f(x)}{g(x)}$$

and say $g(x_0) = 0$

eg. $r(x) = \dfrac{x^2}{x+1}$ $\quad 2 \quad 1$

$x_0 = \infty$

$$r(x) = \frac{\frac{x^2}{x^2}}{\frac{x}{x^2} + \frac{1}{x^2}} = \frac{1}{\frac{1}{x} + \frac{1}{x^2}}$$

$$\frac{}{x^2} + \frac{}{x^2} \qquad \frac{}{x} \quad x$$

if $\mathbb{K} = \mathbb{R}$

$$r(\infty) = \frac{1}{0} = \infty.$$

on the other hand,

$$r(x) = \frac{x}{x^2+1} \qquad \begin{matrix} 1 \\ 2 \end{matrix}$$

$r(\infty) = ?$

$$r(x) = \frac{\frac{x}{x^2}}{\frac{x^2}{x^2} + \frac{1}{x^2}} = \frac{\frac{1}{x}}{1 + \frac{1}{x^2}}$$

$x \to \infty$

$$r(\infty) = \frac{0}{1+0} = 0$$

Lastly, if

$$r(x) = \frac{1 \cdot x^2 + 2}{3 \cdot x^2 + 4x + 1}$$

$$r(\infty) = ?$$

$$r(x) = \frac{\frac{x^2}{x^2} + \frac{2}{x^2}}{3 + \frac{4}{x} + \frac{1}{x^2}}$$

$$x \to \infty$$

$$= \frac{1 + 0}{3 + 0 + 0} = \frac{1}{3}$$

$$T_n \quad k(E) = \left\{ r = \frac{f}{g} \;\middle|\; f, g \in \right.$$

$\mathbb{k}[E]$ }

$r(0)$

We need to define

$\deg(f)$ for $f \in \mathbb{k}[E]$

in E :

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

So we set $\deg(y) = 3$

$\deg(x) = 2$

and

Def: For $f \in \mathbb{k}[E]$ in

canonical form

$$f(x,y) = v(x) + y\,w(x)$$

$$\deg(f) = \max\left\{2\cdot \deg_x(v),\ 3+2\cdot\deg_x(w)\right\}$$

Def: For $r = \frac{f}{g} \in k(E)$ $\left(\begin{matrix} f,g \\ \in k[E] \end{matrix}\right)$

distinguish 3 cases:

1) $\deg f < \deg g$

define $r(0) := 0 \in k$

2) $\deg f > \deg g$

define $r(0) = \infty \in \mathbb{P}^1$

(3) if $\deg f = \deg g$ then

(i) if $\deg f$ is <u>even</u>

where ax^n, bx^n

are the highest

monomials of f, g

respectively

define $r(0) = \frac{a}{b}$.

(ii) if $\deg f = \deg g$ is <u>odd</u>

where $ax^n y$, $bx^n y$

are the highest monomials

of f, g resp.,

define $r(0) = \frac{a}{b}$.

$\Rightarrow$)

$r : E(\mathbb{k}) \longrightarrow \mathbb{P}^$

is an induced function

(before $r : E(\mathbb{k}) \setminus \{O\} \longrightarrow \mathbb{P}^1 - \mathbb{k} \cup \{\infty\}$

$P \xmapsto{\text{reg}} r(P)$

$\xmapsto{\text{ireg}} \infty$)

Example: $\mathbb{k} = \mathbb{R}$, $E : y^2 = x^3 + Ax + B$

$$r(x,y) = \frac{x^3 + 2x + y + 2x^4 y}{x + x^2 + 5xy^3} \in \mathbb{k}(E)$$

We can write $\boxed{2x^4 \cdot y}$

$$r(x,y) = \frac{\overbrace{(x^3 + 2x)}^{} + \overbrace{y(1 + 2x^4)}^{}}{(x + x^2) + y(5x^4 + 5Ax^2 + 5Bx)}$$

$\boxed{5x^4 y}$

$\max\{2 \cdot 3, 3 + 2 \cdot 4\} = 11$

deg : $\max\{2\cdot 2, 3+2\cdot 4\} = 11$

$0 =$ "(∞, ∞)"

then $r(0) = \frac{2}{5}$.

Def: Fix $r \in \mathbb{k}(E)$.

A point $P \in E(\mathbb{k})$ is called

a zero of r

if $r(P) = 0 \in \mathbb{P}^1$

and a pole of r if

$r(P) = \infty \in \mathbb{P}^1$.