Recall

an elliptic curve over k

is an equation

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

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

last time

$\Delta(E) \neq 0 \quad (=)$

"Algebraic" $f(x) = x^3 + Ax + B$

has no repeated roots

in $\overline{k}$

(=)

"Geometric" over $\mathbb{R}$ $\Delta(E) \neq 0$

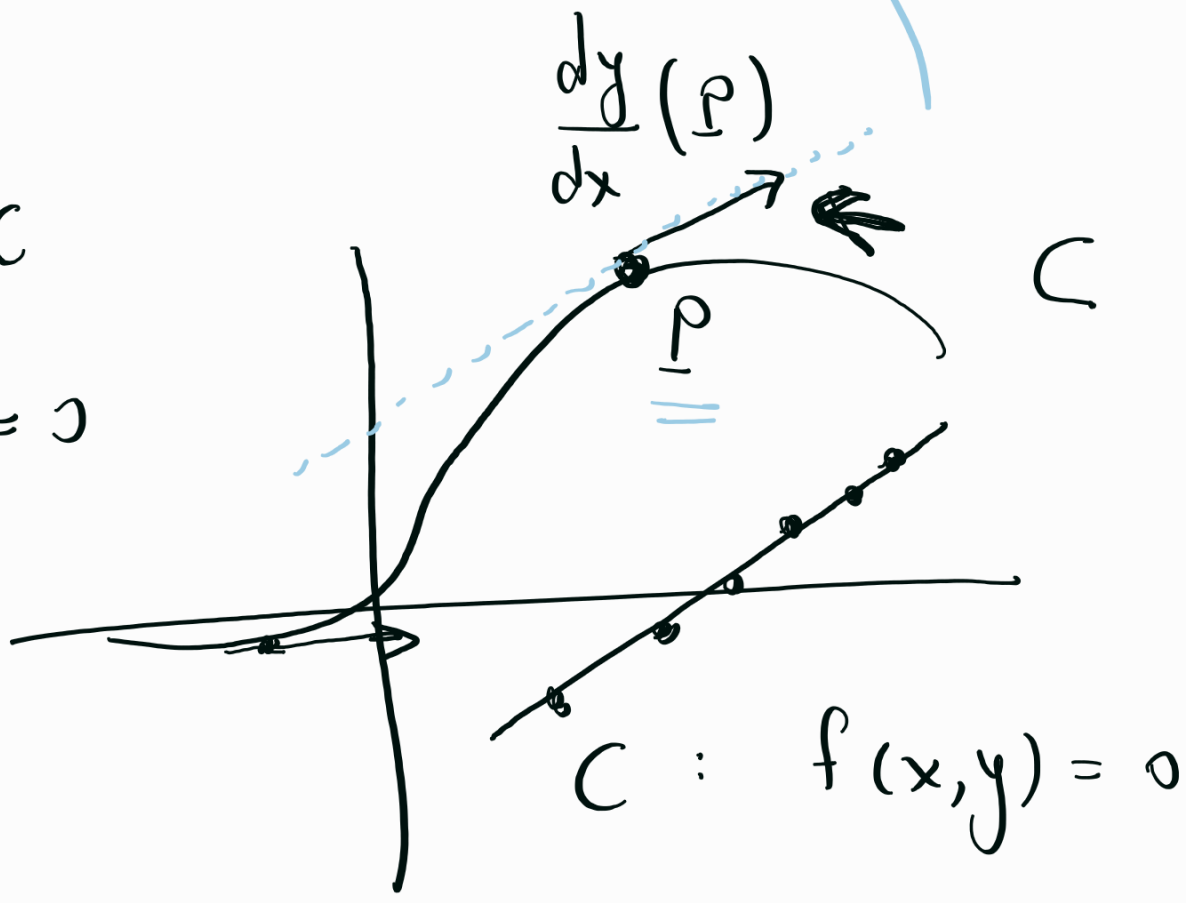
is the same as saying that E has a tangent line at every point "smooth".

In calculus

$P \in C$

$\Leftrightarrow$

$f(P) = 0$



Def: Let $f(x,y)$ be a polynomial over $\mathbb{k}$ and $P = (x_0, y_0) \in \mathbb{k} \times \mathbb{k}$ s.th $f(P) = 0$, then if

$m := \frac{dy}{dx}(P)$ exists, we

define the tangent line to f at $\underline{P}$ as the equation

$$y - y_0 = m(x - x_0)$$

Affine Geometry

$$\mathbb{A}^n_{\mathbb{k}} = \underbrace{\mathbb{k} \times \cdots \times \mathbb{k}}_{n\text{- times}} = \mathbb{k}^n$$

affine plane

$$\mathbb{A}^2 = \mathbb{k}^2 \quad (\hookrightarrow \mathbb{R}^2)$$

a line in $\mathbb{A}^2$ is

the solution set of

$$\{(x,y) \in \mathbb{k}^2 \mid y = mx+b\} \quad \boxed{y = mx + b}$$

where $m, b \in \mathbb{k}$.

Example: $E : y^2 = x^3 + 2x$

$\frac{dy}{dx}$ " $y(x)$ "

$$2y \cdot \frac{dy}{dx} = 3x^2 + 2$$

$$\frac{dy}{dx} = \frac{3x^2+2}{2y}$$

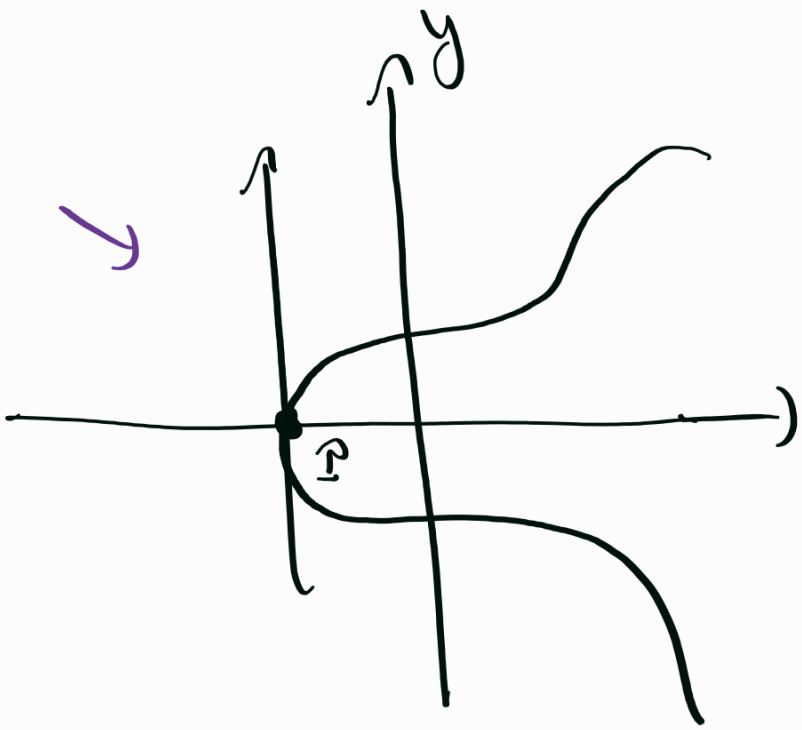
$\frac{dy}{dx}$ " " "

$\frac{dx}{dy}$ $x(y)$

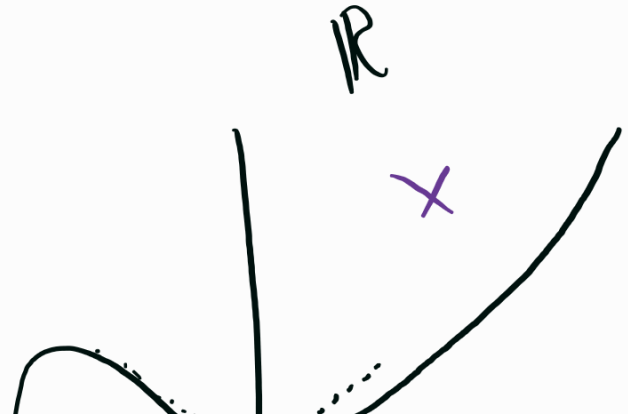
$$2y = 3x^2 \cdot \frac{dx}{dy} + 2\frac{dx}{dy}$$

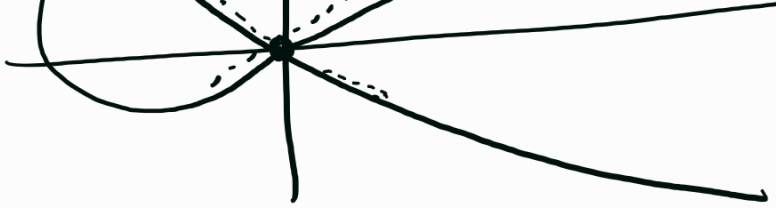
$$\Rightarrow \frac{dx}{dy} = \frac{2y}{3x^2+2}$$

Edge case



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

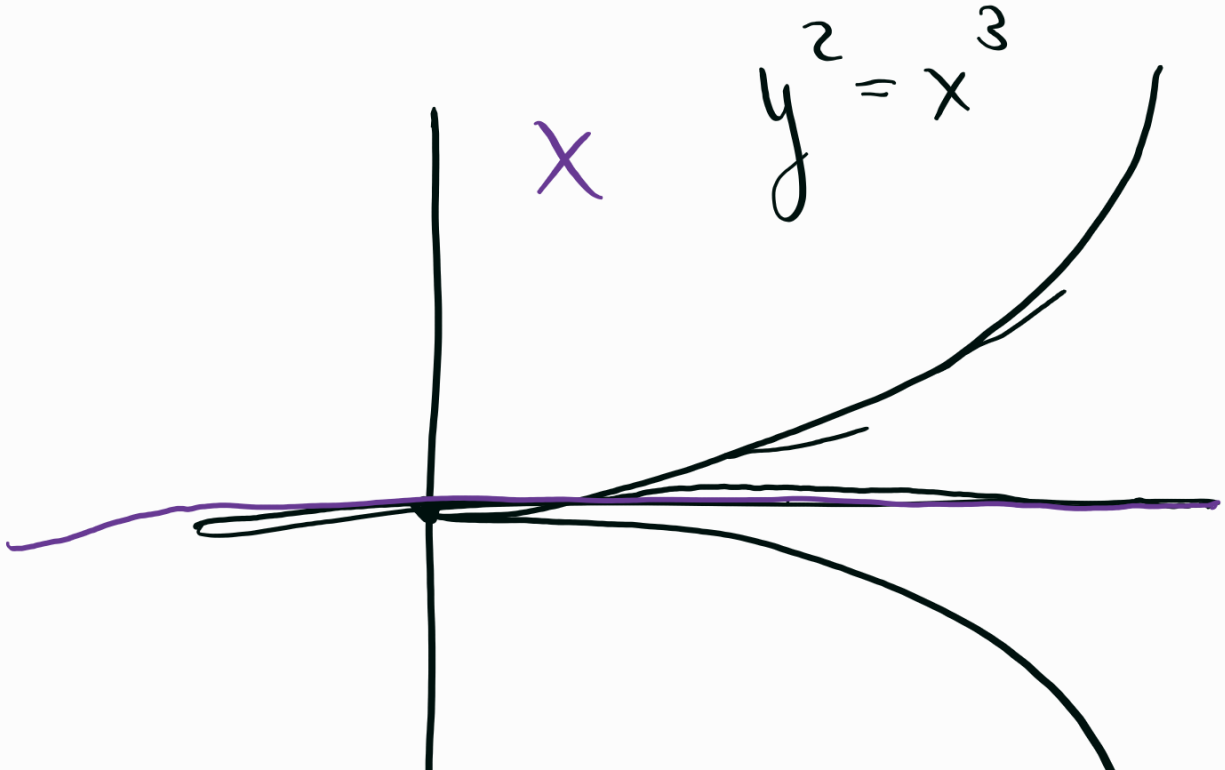




$$2y \cdot \frac{dy}{dx} = 3x^2 + 2x$$

$$\Leftrightarrow \quad \frac{dy}{dx} = \frac{3x^2 + 2x}{2y}$$

$\frac{dy}{dx}(0,0)$ is undefined



$$2y \cdot \frac{dy}{dx} = 3x^2$$

$$\Leftrightarrow \boxed{\frac{dy}{dx}} = \frac{3x^2}{2y}$$

undefined at $(0,0)$.

---

over $\mathbb{R}$ the curve

$C : f(x,y) = 0$ has

a vertical tangent

line at $P = (x_0, y_0)$

if C ... where we subtract

iff when we restrict

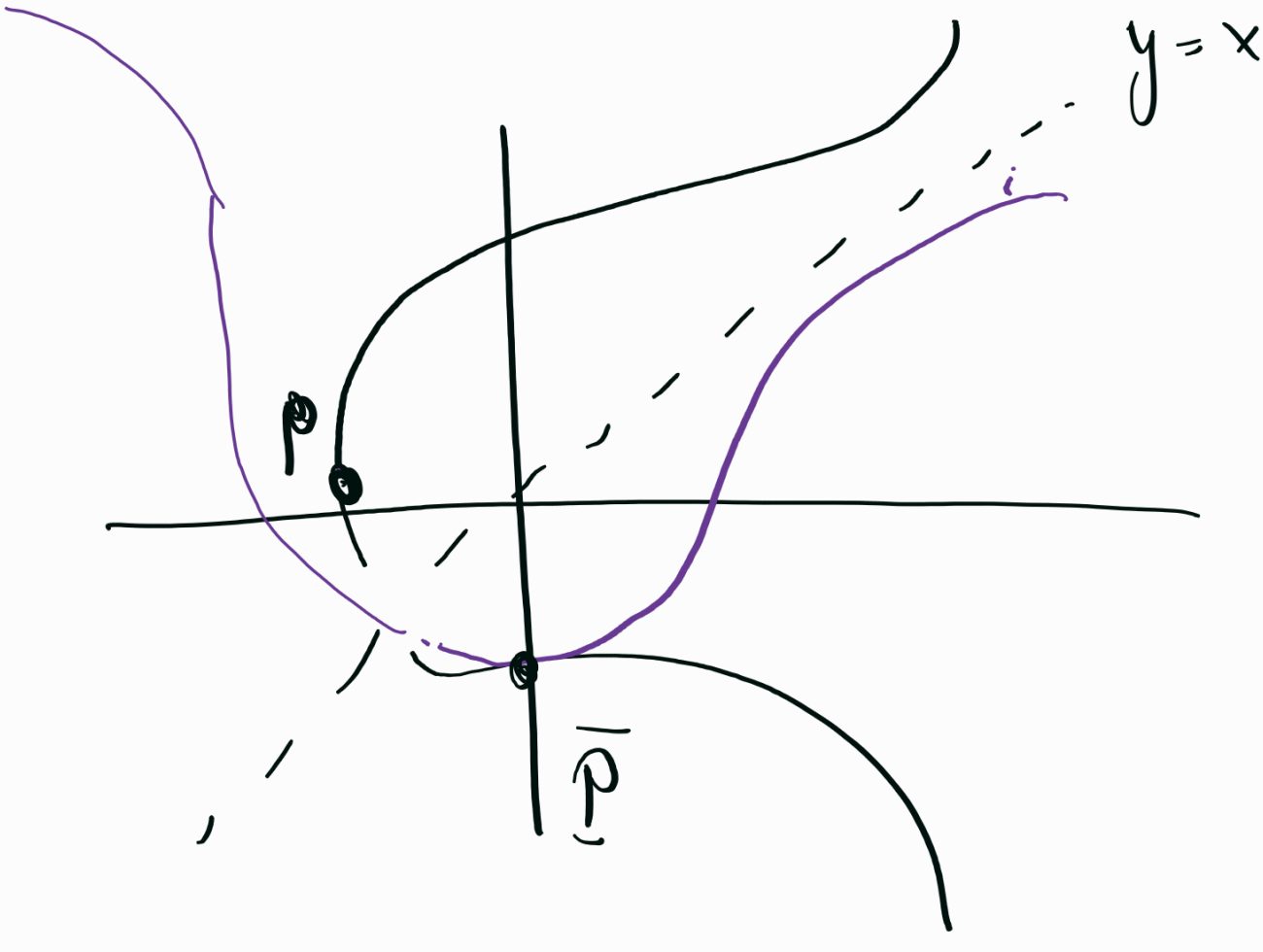
C along the line

$y = x$, the resulting

curve has a tangent

line with slope 0

at $\bar{P} = (y_0, x_0)$



so formally

Def $E : y^2 = x^3 + Ax + B$ / k has a vertical tangent line at $P = (x_0, y_0)$ if

$$\frac{dx}{dy}(P) = 0$$

(then the equation of the tangent line is $x = x_0$)

Def: A curve $C: f(x,y) = 0$ over k is smooth if it has a tangent line at every point.

Proposition: Let k be a field and $E: y^2 = x^3 + Ax + B$ a curve over k. Then

E is an elliptic curve iff it is smooth.

In other words,

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

iff $\exists$ a tangent line

at every point P on E.

"(x_0, y_0)

Proof: Taking Implicit derivation

$$\frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

$$\frac{dy}{dx}(x_0, y_0) = \frac{\to 3x_0^2 + A}{\to 2y_0}.$$

If $y_0 \neq 0$ we have

a tangent line at P.

Suppose $y_0 = 0$ but $3x_0^2 + A \neq 0$

Then $\frac{dx}{dy} = \frac{2y}{3x^2 + A}$

and E has a vertical tangent line at P.

Lastly, if $y_0 = 0$ and $3x_0^2 + A = 0$

then necessarily, $A < 0$

and we can substitute $A = -A$ to get

$$3x_0^2 - A = 0 \quad , \quad A > 0$$

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

↳ 3

Since $x_0^3 - Ax_0 + B = 0$

we get

$$\left(\sqrt{\frac{A}{3}}\right)^3 - A\sqrt{\frac{A}{3}} + B = 0$$

$$\frac{2A^{3/2}}{3\sqrt{3}} = B \quad / (\,)^2$$

$$\Leftrightarrow \quad \frac{4A^3}{27} = B^2$$

$$\Leftrightarrow \quad \boxed{4A^3 - 27B^2 = 0}$$

Substitute back $A = -A$

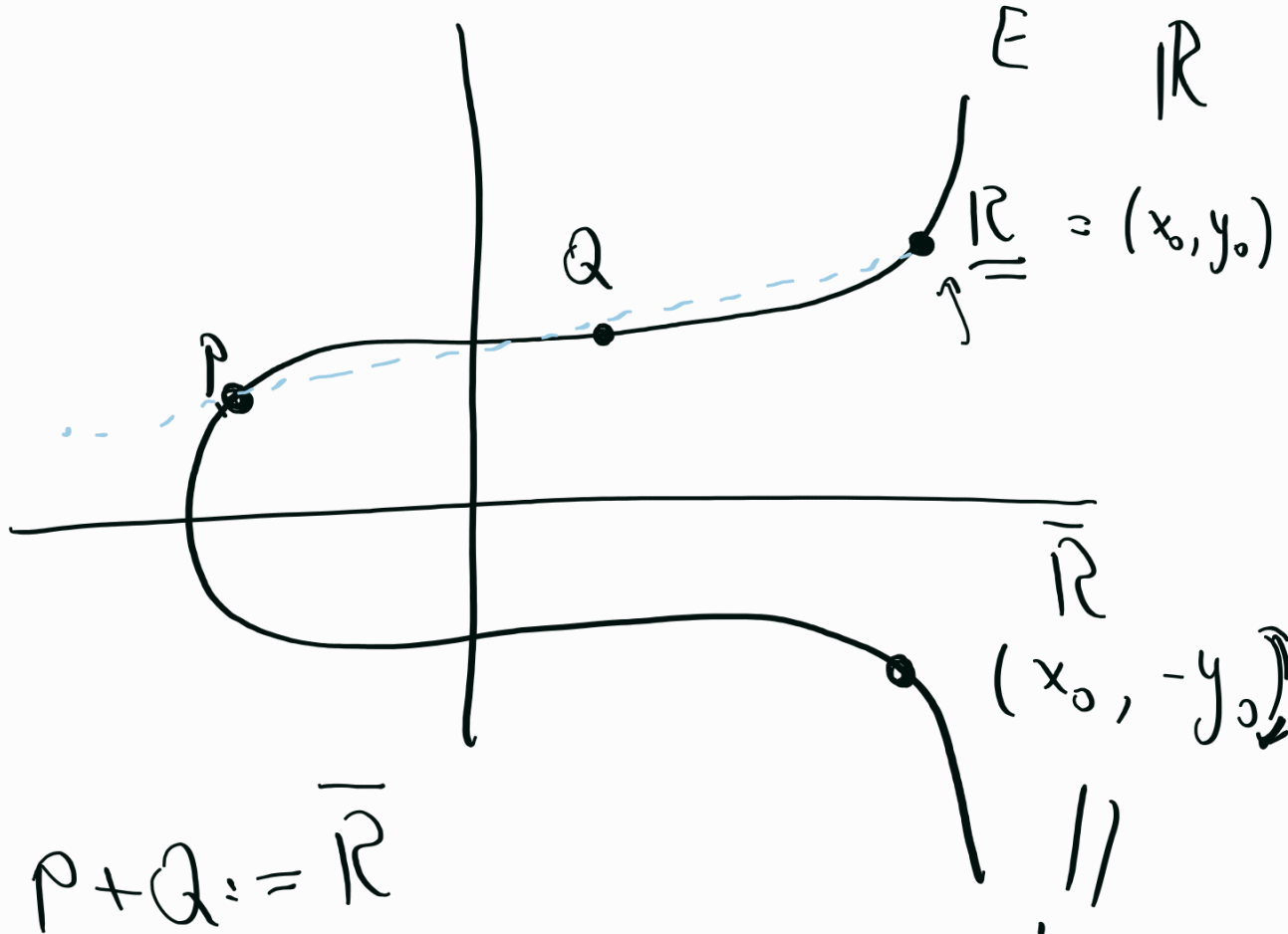
$(\Leftarrow)$ $4A + 27B = 0$

$\Updownarrow$

$\Delta(E)$

so there is a tangent line in this case $(\Leftarrow)$

$\Delta(E) \neq 0.$ //



$P + Q := \bar{R}$

//

$P + Q$

$P + P = \bar{R}$

$\infty = "0"$

$\Rightarrow$

$\Rightarrow \quad P + P = \infty$

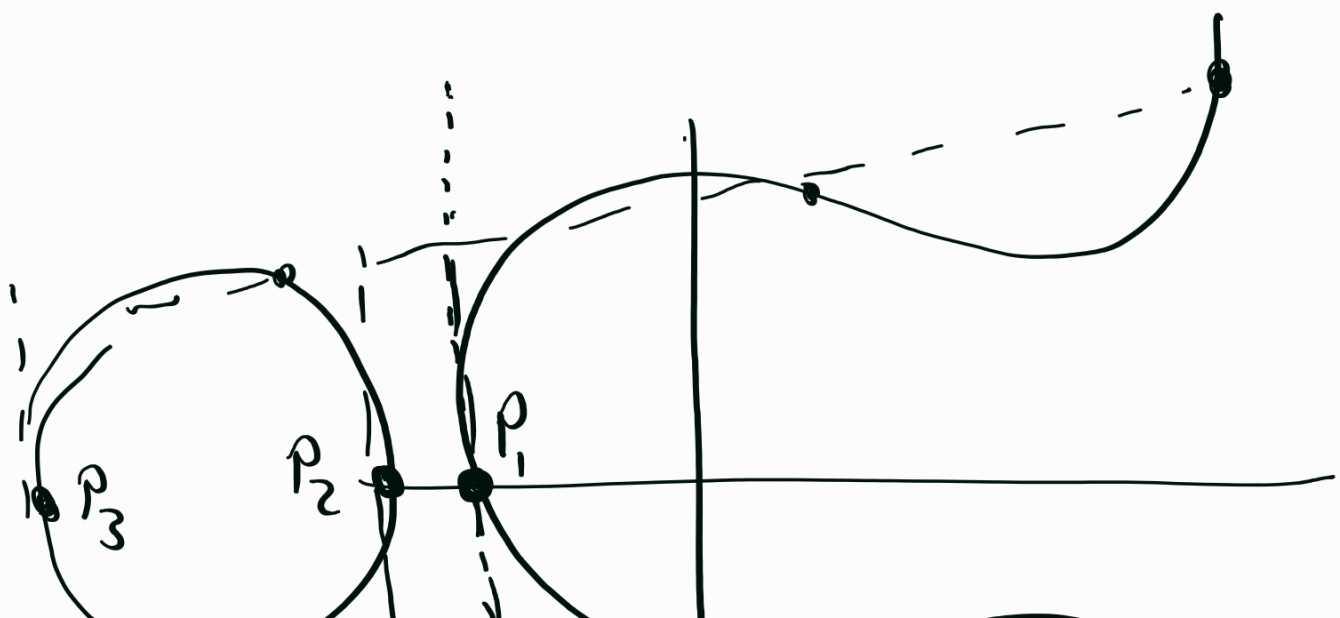
Def: Let E/k be an elliptic curve. The set of k-rational points is

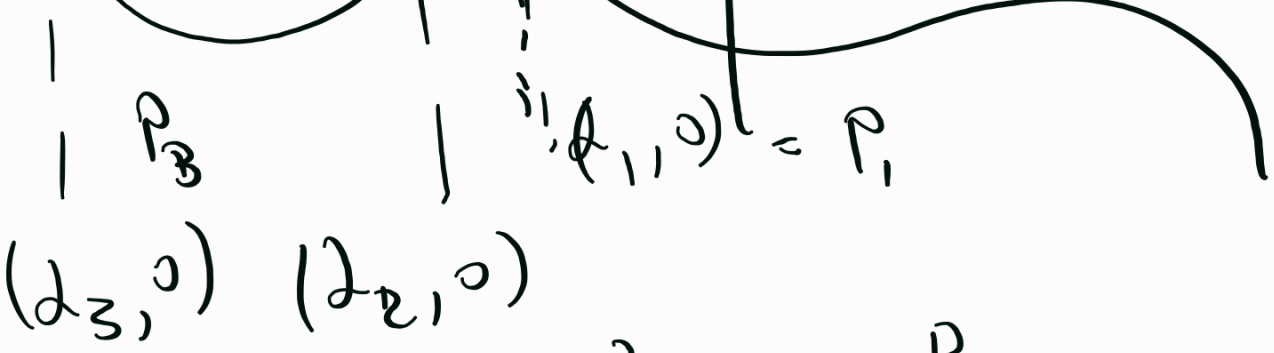
$$E(k) = \{(x,y) \mid y^2 = x^3 + Ax + B\}$$

$$\cup \{O\}$$

$P_i + P_i = O$

$\mathbb{R}$





$$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$