Wed, Oct 1, 2014

We'll talk about A_n and simplicity another time.

Today: elliptic curves.

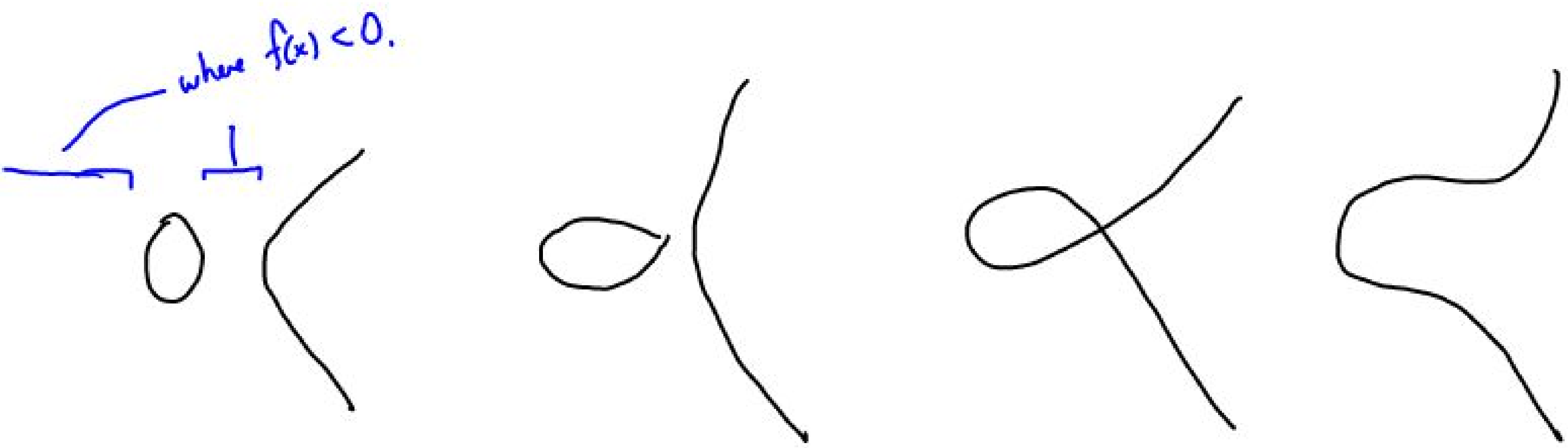
<u>**Defn**</u> Let $f(x)$ be a nice cubic polynomial in x.

TBD.

The <u>elliptic</u> <u>curve</u> <u>defined</u> <u>by</u> <u>f</u> (for this class) is the set

$$\{\mathcal{O}\} \cup \{(x,y) \mid y^2 = f(x)\} =: \mathbb{E}$$

<u>Ex</u> The solutions to $y^2 = f(x)$ look like



Singular.
$f(x)$ is NOT nice.

Note $(x,y) \in \mathbb{E}$
$\Longrightarrow (x,-y) \in \mathbb{E}$.

<u>**Thm**</u> Every elliptic curve is an abelian group.

This is quite surprising. Let me define for you the group operation

$$\mathbb{E} \times \mathbb{E} \longrightarrow \mathbb{E}$$
$$(P, \quad Q) \longmapsto P+Q$$

(1) If $P, Q = \mathcal{O}$, then we set

$$\mathcal{O} + \mathcal{O} = \mathcal{O}.$$

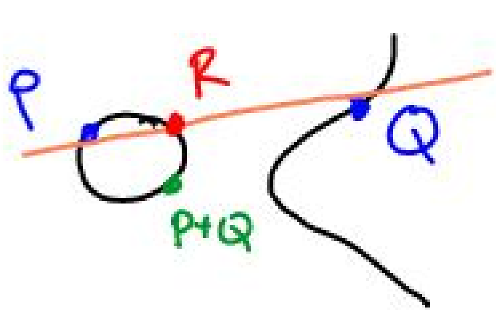
making $\mathcal{O}$ identity. Nothing special

(2) If $P = \mathcal{O}$, $Q = (x, y) \in \mathbb{E}$, we set

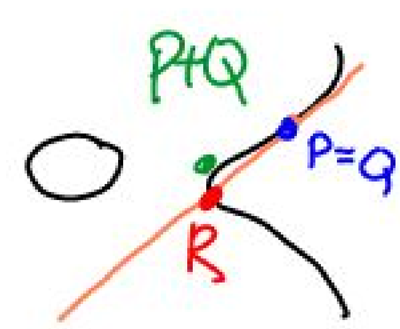
$$\mathcal{O} + Q = Q + \mathcal{O} = Q.$$

(3) If P, Q are on $\{(x,y) \mid y^2 = f(x)\}$:

Consider the (unique!) line L_{PQ} containing P and Q.



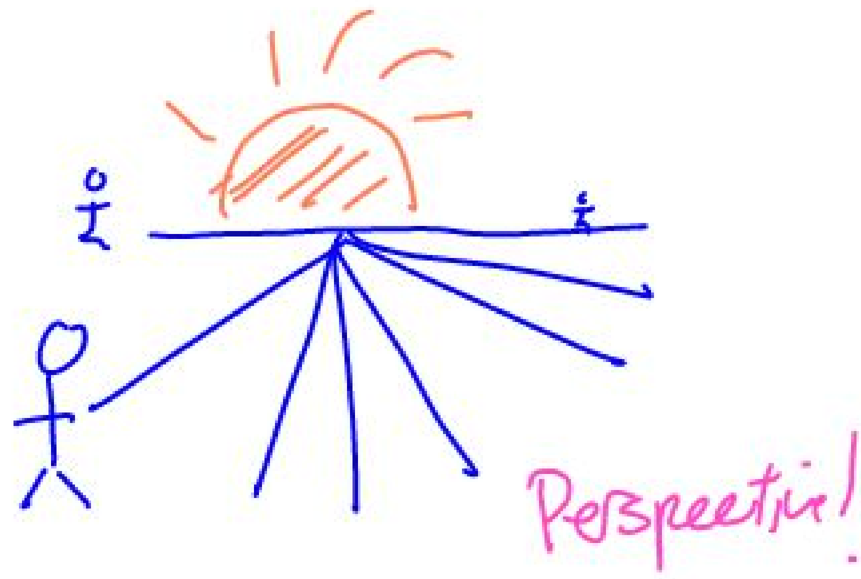
If $P = Q$, we take tangent to P.

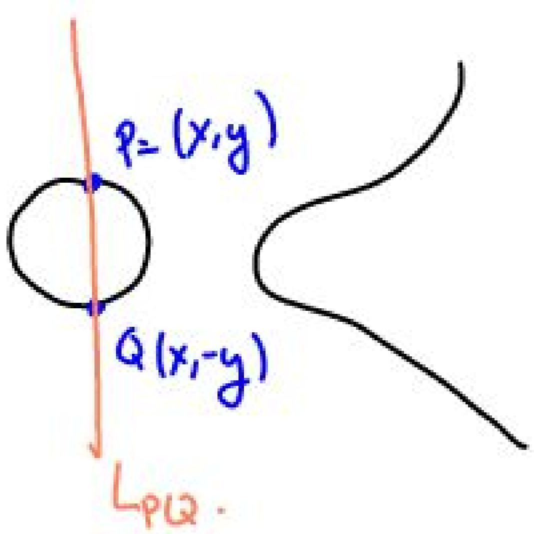


A line L intersects a cubic in three points. Let $R = (x, y)$ be the third. Then we define $P+Q := (x, -y)$.

Rules: If L_{PQ} is vertical, so it doesn't intersect a 3rd pt in $\mathbb{R}^2$, we declare the 3rd pt R to be the "point @ ∞," $\mathcal{O}$.

(This isn't really a rule, but rather an interpretation using projective geometry, where parallel lines — like vertical lines — intersect at a pt @ ∞.)





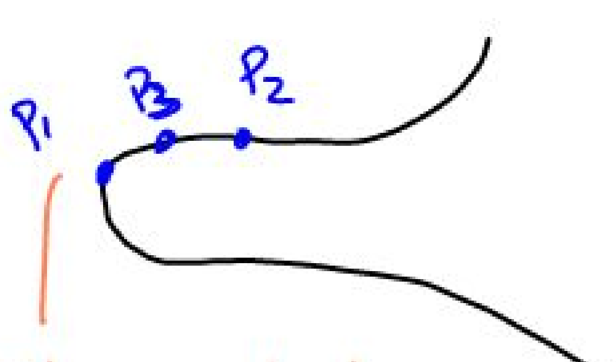
$P+Q = \mathcal{O}$ in this case.

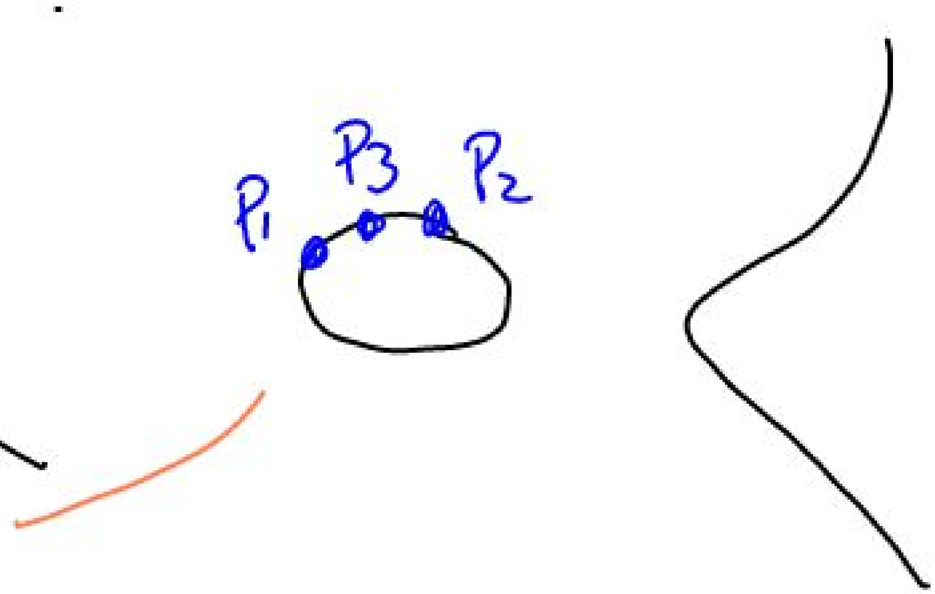
So $Q = -P$.

Note $L_{PQ} = L_{QP}$, so $P+Q = Q+P$. Hard to prove: $\mathbb{E} \times \mathbb{E} \to \mathbb{E}$ is associative. Try it!

Activity time: Prove

$$(P_1+P_2)+P_3 = P_1+(P_2+P_3).$$





I'd recommend choosing 3 pts near each other.

Awesome observation:

Assume $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ has $a_i, b \in \mathbb{Q}$. Suppose $P, Q \in \mathbb{E}$ are <u>rational</u> points (meaning their x- and y-coordinates are rational numbers). Then $P+Q$ is <u>also</u> a rational point!

<u>Pf</u>: L_{PQ} is given by

$$y = mx + t.$$

$P, Q \in \mathbb{Q} \Rightarrow m, t \in \mathbb{Q}$.

$L_{PQ} \cap \mathbb{E} \ni R$ satisfies equation

$$(mx+t)^2 = a_3x^3 + a_2x^2 + a_1x + a_0$$

$\Rightarrow P, Q, R$ are roots to some cubic $g(x)$ w/ rational coefficients.

$$\Rightarrow (x - x_P)(x-x_2)(x-x_3) = g(x) = b_3x^3 + b_2x^2 + b_1x + b_0.$$

But $x_1, x_2 \in \mathbb{Q} \Rightarrow x_3 \in \mathbb{Q}$, since $x_1x_2x_3$ is constant term of $g(x)$!

(Better: since $x_1 + x_2 + x_3 = b_2$, and $x_1, x_2, b_2 \in \mathbb{Q}$.)

//

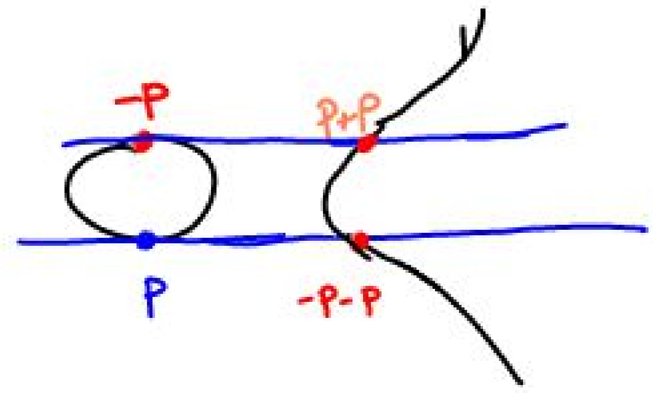
<u>Defn</u> If f is a rational cubic (i.e., $a_i \in \mathbb{Q}$) let $\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}$ denote the set

$$(\mathbb{E} \cap (\mathbb{Q} \times \mathbb{Q})) \cup \{O\}.$$

(ie, the set of all P s.t. the coordinates of P are rational numbers, along w/ the point at ∞.)

So we have a subset

$$\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}.$$



It's closed under $+$.

It's closed under inverses, since $P = (x, y) \in \mathbb{Q} \times \mathbb{Q}$

$$\Longrightarrow -P = (x, -y) \in \mathbb{Q} \times \mathbb{Q}.$$

And $\mathbb{E}(\mathbb{Q}) \ni \mathcal{O} =$ identity by def'n. So we see

<u>Prop'n</u> $\mathbb{E}(\mathbb{Q}) \subset \mathbb{E}$ is a subgroup.

Digression:

<u>Def'n</u> G is called <u>finitely generated</u> if $\exists$ a finite set S and a surjective homomorphism

$$F(S) \longrightarrow G.$$

Parsing this definition:

Let $S = \{s_1, \cdots, s_n\}$ be the finite set, and

$$\phi : F(S) \longrightarrow G$$

the onto homomorphism.

ϕ sends each s_i to some element $g_i = \phi(s_i)$.

That ϕ is onto means that $\forall\, g \in G$, $\exists$ a word w s.t.

$$\phi(w) = g$$

i.e., g can be written as a finite product of the g_i and the g_i^{-1}.

So the down-to-earth meaning is that $\exists$ some finite collection

$$g_1, \cdots, g_n \in G$$

s.t. any element of G can be expressed as a product of the g_i and their inverses.

Ex

Any finite group G is finitely generated. Take

$$S = G$$

and map

$$\underbrace{F(S)}_{\text{huge, infinite group!}} \longrightarrow G.$$

$$g \longmapsto g.$$

Ex Any cyclic group is finitely generated. If

$$G = \langle g \rangle,$$

set $S = \{g\}$,

$$F(S) \longrightarrow G$$

$$g \longmapsto g.$$

Ex Any finite product of fin. gen. groups is again finitely generated:

$$G = G_1 \times \cdots \times G_n.$$

Take generating sets S_i for G_i, and define $S = S_1 \cup \cdots \cup S_n$.

If $\phi_i : F(S_i) \longrightarrow G_i$ is a surjection $\forall i$, let

$$\phi : F(S) \longrightarrow G$$

$$\underset{\overset{\cap}{S_i}}{a_i} \longmapsto (1, \dots, 1, \underset{\overset{\cup\!\!\!\cup}{G_i}}{\phi_i(a_i)}, 1, \dots, 1).$$

One of the most important theorems about elliptic curves is

<u>Thm</u> (Mordell's Theorem)
$\mathbb{E}(\mathbb{Q})$ is finitely generated.

Crazy surprising — there's some <u>finite</u> collection of rational points $P_1, \dots, P_n \in \mathbb{E}(\mathbb{Q})$ such that any other rational point can be obtained by <u>adding + subtracting</u> the P_i from each other.

using the group operation.