Introduction to Elliptic Curves

Let K be a field.

Projective coordinates

$$\mathbb{P}^2(K) = \left\{ (a,b,c) \;\middle|\; \begin{array}{l} a,b,c \in K \\ (a,b,c) \neq (0,0,0) \end{array} \right\} \Big/ \sim$$

(Projective space)

$$(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$$

$$\Longleftrightarrow \quad (a_2, b_2, c_2) = \lambda (a_1, b_1, c_1) \quad \lambda \in K - \{0\}$$

Remark: 1) This 2 can be replaced by any natural number.

2) In some general settings, we can talk about weighted projective space

[e.g.

$$a_2 = \lambda^a a_1 \qquad a \neq b \neq c$$
$$b_2 = \lambda^b b_1$$
$$c_2 = \lambda^c c_1$$

$$\mathbb{P}^2(K) = \left\{ (a,b,c) \;\middle|\; \begin{array}{l} (a,b,c) \neq (0,0,0) \\ a,b,c \in K \end{array} \right\} \Big/ \sim$$

Choose $(a,b,c) \in \mathbb{P}^2(K)$

$c \neq 0$

$\left(\frac{a}{c}, \frac{b}{c}, 1\right)$

$\wr\wr$

$\mathbb{A}^2(K) = \{(x,y) \mid x,y \in K\}$

(affine space)

$c = 0$

$(a,b) \sim \mathbb{P}^1(K)$

$$\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \mathbb{P}^1(K)$$

In general we would have that

$$\mathbb{P}^n(K) = \mathbb{A}^n(K) \cup \mathbb{P}^{n-1}(K)$$

Assume further that char $(K) \neq 2$ or 3

Recall Char (K) is the smallest positive number n such that $\underbrace{1+1+\cdots+1}_{n} = 0$

Defn: An elliptic curve $E \subseteq \mathbb{P}^2(K)$ is given by an equation of the form

$$y^2 = x^3 + ax + b \qquad a, b \in K$$

Such that x^3+ax+b has distinct roots.

Example: x^2-2, Roots of x^2-2 are $\sqrt{2}, -\sqrt{2}$

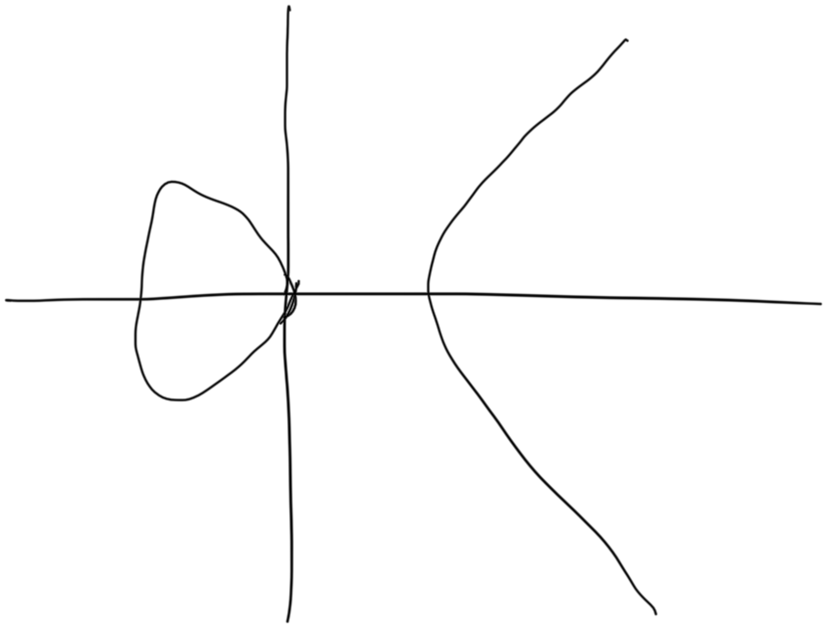
Examples of Elliptic Curves

$$E_1 := y^2 = x^3 - x \qquad \text{over } \mathbb{R}$$

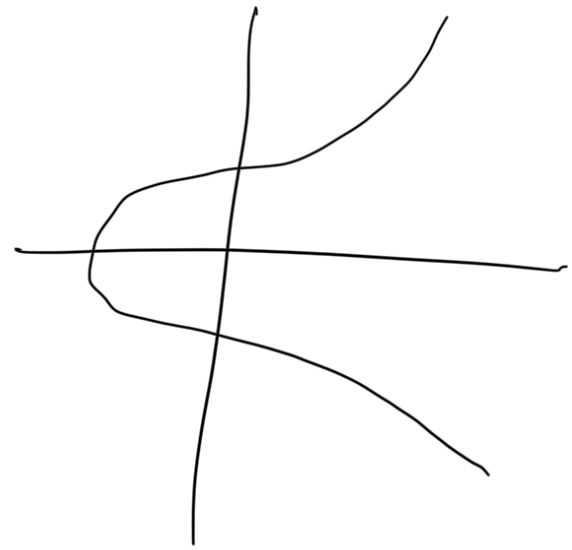
$$= x(x^2-1) = x(x-1)(x+1)$$

$$E_2 := y^2 = x^3 + x/4 + 5/4$$

ε_1



ε_2



Take projective coordinates

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

$$\boxed{(x, y, z) \sim \left(x/z,\, y/z,\, 1\right)}$$

$$\frac{y^2}{z^2} = \frac{x^3}{z^3} + \frac{ax}{z} + b$$

$$\frac{y^2}{z^2} = \frac{x^3 + axz^2 + bz^3}{z^3}$$

$$zy^2 = x^3 + axz^2 + bz^3$$

If $z=0$

$$0 = x^3 \Rightarrow x=0$$

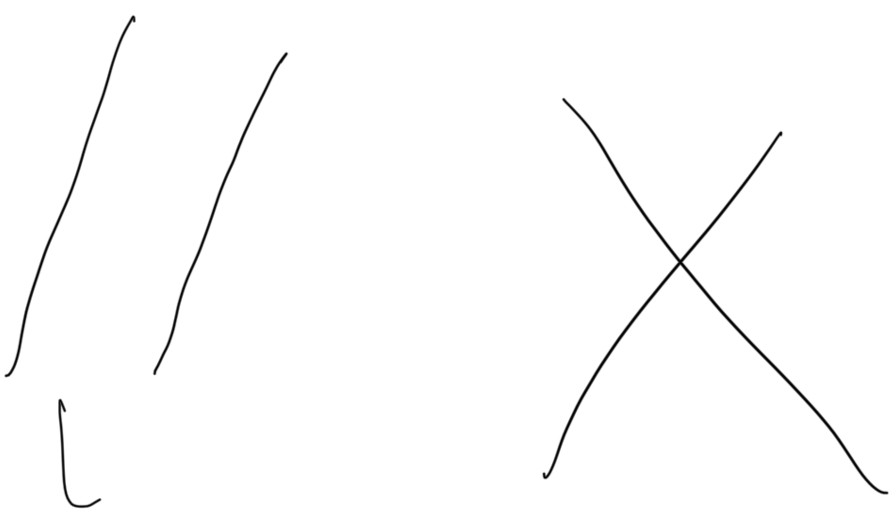
$(0, y, 0) \sim (0,1,0)$ — Point at infinity

(we will denote it by ∞.)

<u>Aside</u> Why do we care about projective spaces?

Geometry is simple over projective spaces.

Let's take example of two lines

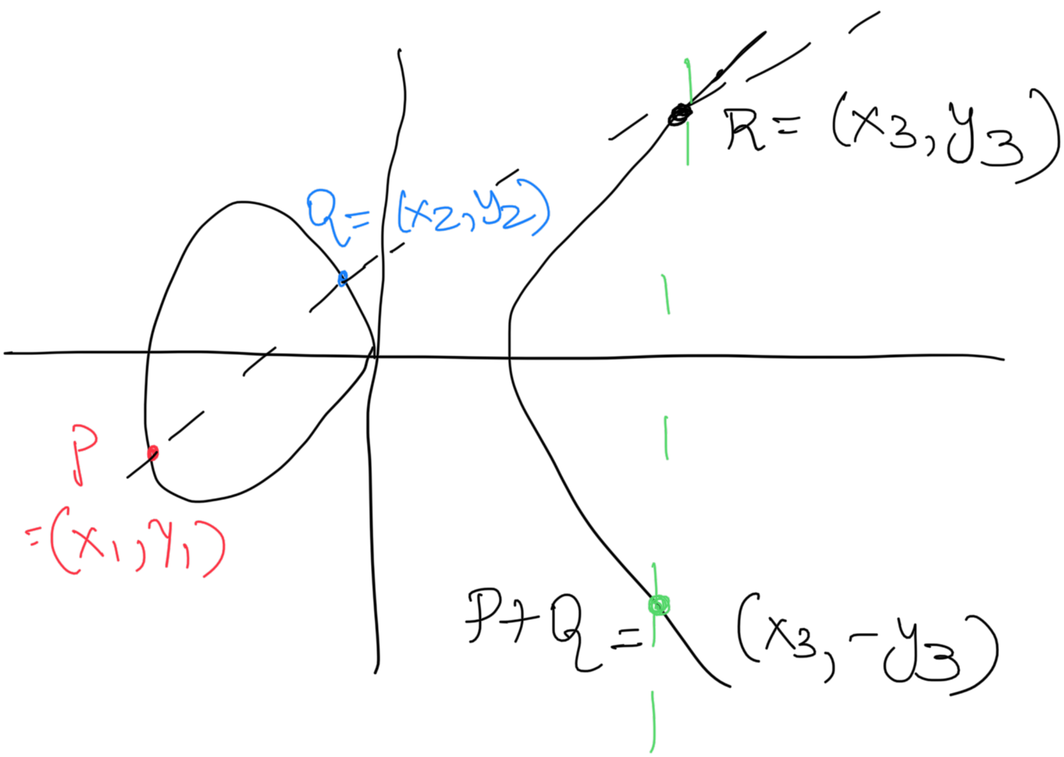


In projective space these lines meet at infinity

Bezout's thm: A curve of degree m & a curve of degree n intersect at mn points.

$$y^2 = x^3 + ax + b \qquad \infty$$

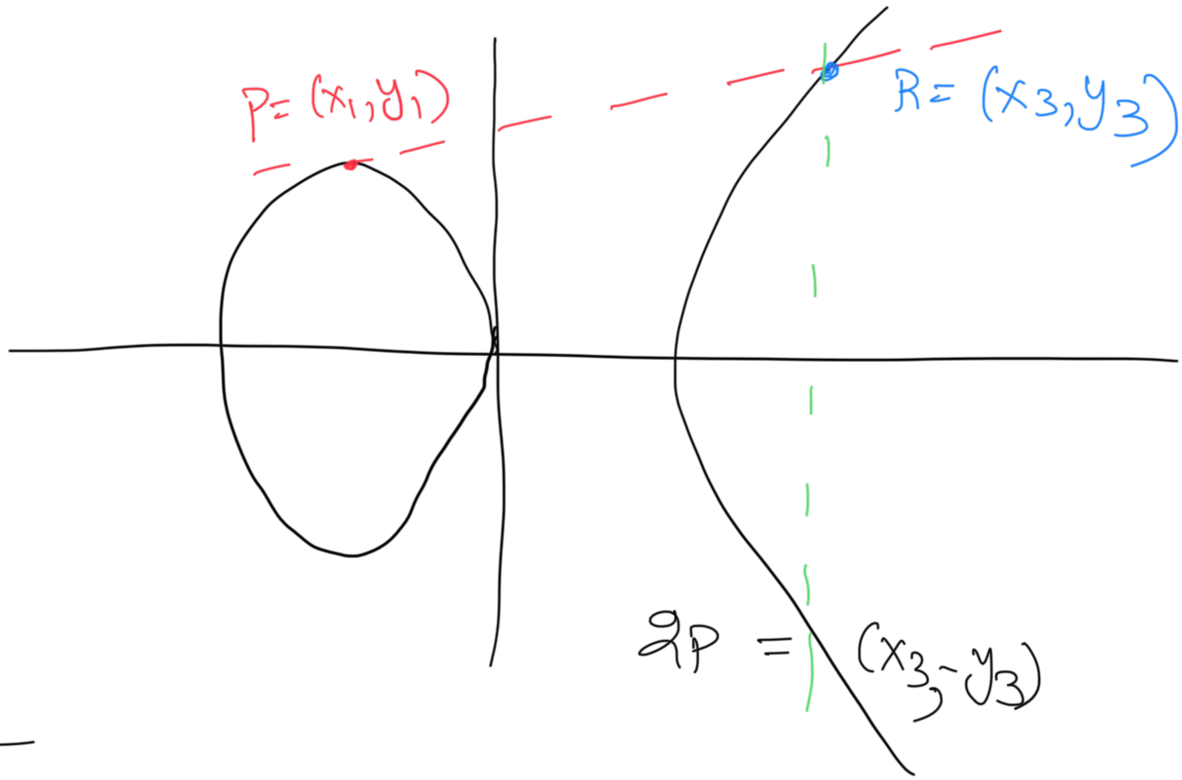
We can add two points on elliptic curves.



Chord law of addition

If $P = Q$ & $P \neq -Q$

$\boxed{P + (-P) = \infty}$



With respect to this addition, $E(K)$ is a group.

1) Associative
2) Identity $\rightarrow \infty$
3) Inverses $\rightarrow$ exist!
4) Commutative

$E(K)$ is an abelian group.

Thm: $\mathcal{E}(K) \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2 \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z}$

$r = \text{rank}(\mathcal{E})$

Explicit equations for addition

$\mathcal{E}: y^2 = x^3 + ax + b$ — (1)

$P = (x_1, y_1)$

$Q = (x_2, y_2)$

Let L be the line joining P & Q.

$$L: = (y - y_1) = \underbrace{\left(\frac{y_2 - y_1}{x_2 - x_1}\right)}_{= m}(x - x_1)$$

$$y = m(x - x_1) + y_1 \quad — (2)$$

Plug in (2) into (1)

$$m^2(x - x_1)^2 + y_1^2 + 2m(x - x_1)y_1 = x^3 + ax + b \quad — (3)$$

Coefficient of x^2 = $-$(Sum of roots)

Let's find out coefficient of x^2 in ③

$$-m^2 = -(x_1 + x_2 + x_3)$$

$$x_3 = m^2 - x_1 - x_2$$

$$\boxed{x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2}$$

Using eqn 2

$$y_3 = m(x_3 - x_1) + y_1$$

$$\boxed{-y_3 = m(x_1 - x_3) - y_1}$$

$$P + Q = (x_3, -y_3)$$

Equation for 2P

To find out slope of tangent, we need to take derivative

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

$$2yy' = 3x^2 + a$$

$$m = y' = \frac{3x^2+a}{2y}$$

$$X_{2p} = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1$$

$$y_{2p} = \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - X_{2p}) - y_1$$

Some explicit calculations

$$\mathcal{E} := y^2 = x^3 + 4x + 6 \qquad \mathbb{F}_7$$

$$\mathcal{E}(\mathbb{F}_7) = \{\infty, (1,2), (1,5), (2,1), (2,6), (4,3), (4,4), (5,2), (5,5), (6,1), (6,6)\}$$

x	x^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

$x=1$

$$y^2 = 1+4+6 = 4$$

$(1,2)$ $(1,5)$

$x=3$

$$y^2 = 27+12+6 = 3$$

$$|\mathcal{E}(\mathbb{F}_7)| = 11$$

$$(2,1) + (4,3) = (2,6)$$

$$(2,1) + (2,1) = (4,4)$$

Observations: $E(\mathbb{F}_7)$ is cyclic.

Proposition: Let G be a finite group. If $|G| = p$ (prime), then G is cyclic.

Pf: Choose $g \in G$ s.t $g \neq e$

$$\langle g \rangle = \{g, g^2, g^3, g^4, \ldots\} \subseteq G$$

$$|\langle g \rangle| \;\Big|\; |G|$$

$$|\langle g \rangle| = |G|$$

$$\langle g \rangle = G.$$