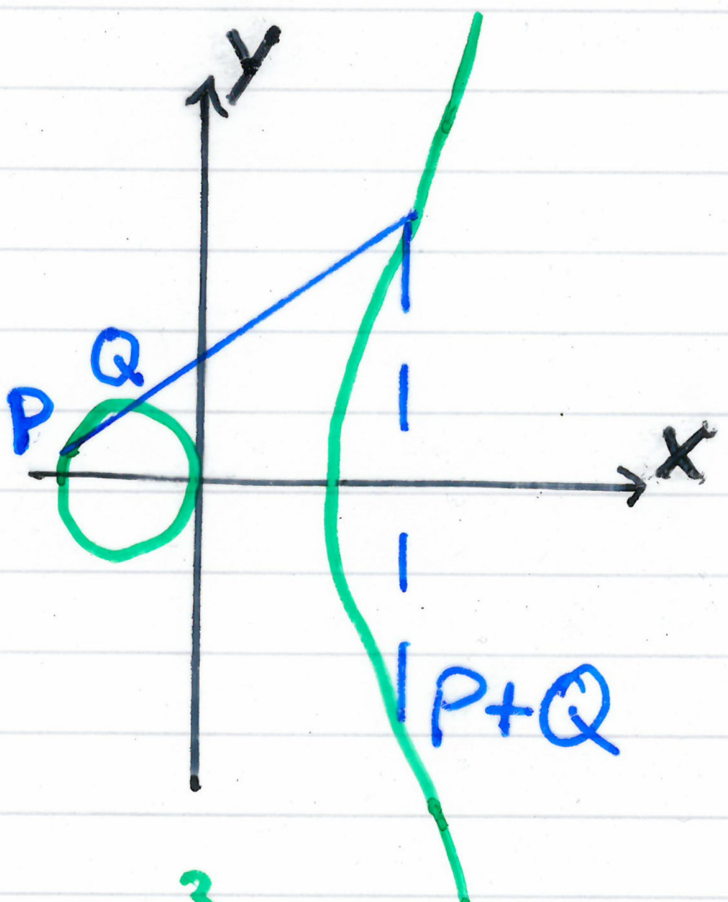
Elliptic curves

We fix K as one of the fields $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Q}$ (rational numbers), $\mathbb{F}_{p^r}$ (finite field of p^r elements), $p > 3$ prime.

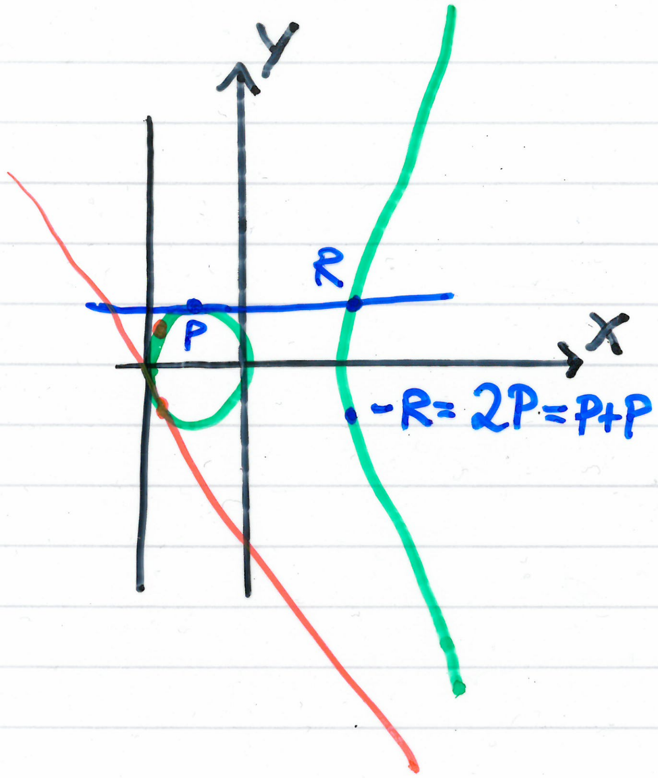
Definition. Let $x^3 + ax + b$ with $a, b \in K$ be a cubic polynomial without multiple roots. An elliptic curve over K is the set of points (x,y) with $x, y \in K$ which satisfy the equation

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

together with a single element denoted O and called the „point at infinity".



$y^2 = x^3 - x$ over $\mathbb{R}$



Definition. We define the sum of two points P and Q on an elliptic curve by the following rules.

1.) If $P=O$, then $-P:=O$ and $P+Q:=Q=:O+Q$

If P and Q are not O:

2.) For $P=(x,y)$, set $-P=-(x,y)\boxed{:=(x,-y)}$.

3.) If $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ with $x_1\neq x_2$, then $R:=$(intersection of $\overline{PQ}$ with elliptic curve), and $P+Q:=-R$.

4.) If $Q=-P$, then $P+Q:=O$.

5.) If $Q=P$, then $R:=$(intersection of tangent line to P with elliptic curve), $R:=P$ if no intersection. $P+P:=-R$.

Coordinate description of addition on elliptic curves

Let $(x_1, y_1) := P$, $(x_2, y_2) := Q$, $(x_3, y_3) := P+Q$

We want to express x_3 and y_3 in terms of x_1, x_2, y_1, y_2.

$\boxed{\text{Case 3: } x_1 \neq x_2}$. Let $y = \alpha x + \beta$ be the equation of the line ℓ through P and Q. Then,

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \beta = y_1 - \alpha x_1.$$

A point $(x, \alpha x + \beta)$ of ℓ lies on $y^2 = x^3 + ax + b$ if and only if

$$(\alpha x + \beta)^2 = x^3 + ax + b.$$

We know that P and Q lie on ℓ; as the equation is of degree 3, there is a third solution:

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

$$y_3 = -(\alpha x_3 + \beta) = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)$$

Example. On the elliptic curve $y^2 = x^3 - 36x$, add $P = (-3, 9)$ and $Q = (-2, 8)$: $P+Q = (6,0)$:

$$x_3 = \frac{(8-9)^2}{(-2-(-3))^2} - (-3) - (-2) = 6, \quad y_3 = -9 + \frac{-1}{1}(-3-6) = 0.$$

Multiples of points on elliptic curves

Let $P=(x_1,y_1)$. Then what is $P+P =: (x_3,y_3)$?

$\boxed{\text{Case 5: } Q=P.}$ The tangent line to P has slope $\alpha = \frac{dy}{dx}$, which we obtain by implicit derivation of the elliptic curve equation $y^2 = x^3+ax+b$.

$$2y\frac{dy}{dx} = 3x^2+a \Rightarrow \alpha = \frac{3x_1^2+a}{2y_1}$$

additional to P itself

The solution to the equation intersecting the tangent line to P with the elliptic curve,

$x_3 = \alpha^2 - x_1 - x_1$, then becomes

$$\boxed{\begin{aligned} x_3 &= \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ y_3 &= -y_1 + (x_1-x_3)\cdot\left(\frac{3x_1^2+a}{2y_1}\right). \end{aligned}}$$

Example. On the elliptic curve $y^2 = x^3-36x$, compute $P+P$ for $P=(-3,9)$. Note: $a=-36$.

$$x_3 = \left(\frac{3(-3)^2+(-36)}{2\cdot 9}\right)^2 - 2(-3) = \frac{1}{4}+6$$

$$y_3 = -9 + \left(-3-\left(\frac{1}{4}+6\right)\right)\cdot\left(\frac{3(-3)^2+(-36)}{2\cdot 9}\right) = \frac{-72+37}{8}$$

Exercise: Addition on the curve $y^2 = x^3 - 36x$

Complete the following table.

P	Q	$P+Q$	$P+P =: 2P$	$Q+Q = 2Q$
$(-3,9)$	$(-2,8)$	$(6,0)$	$\left(\frac{25}{4}, \frac{-35}{8}\right)$	

$P+2P$	$P+2Q$	$Q+2P$	$2P+2Q$

$(P+Q)+(P+Q)$	$P+(P+Q)$	$Q+(P+Q)$

Beware of the fact that any point with $\frac{1}{0} = \infty$ in one of its coordinates is identical to the horizon O.