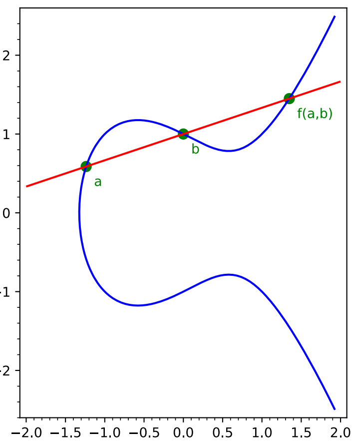
Presence Sheet 6

Exercise 1. Consider the (irreducible) affine curve

$$X^0 = V(x_2^2 - x_1^3 + x_1 - 1) \subseteq \mathbb{A}^2_{\mathbb{C}}\,.$$

a) What are the points in the projective closure $X = \overline{X}^0 \subseteq \mathbb{P}^2_{\mathbb{C}}$?
Note: The curve X is an example of an *elliptic curve*.

b) Given $a, b \in X$ with $a \neq b$, there is a unique line $L_{ab} \subseteq \mathbb{P}^2_{\mathbb{C}}$ through a, b, which intersects X in a third point $f(a,b)$, counted with multiplicity.



Compute $f(a,b)$ for

i) $a = (1 : -1 : 1)$ and $b = (1 : 0 : 1)$

ii) $a = (1 : 0 : 1)$ and $b = (0 : 0 : 1)$

c) Show that $U = \{(a,b) \in X \times X : a \neq b\}$ is an open subset of $X \times X$.
Hint: Using results from the lecture, there is a one-sentence argument for this!

d) *Optional:* Show that the map $U \to X, (a,b) \mapsto f(a,b)$ is a morphism.

Fact: The morphism $f : U \to X$ extends uniquely to a morphism $f : X \times X \to X$. Then we can define a group structure $(X, \oplus, e)$ on X which is uniquely determined by the property that $e = (0 : 0 : 1)$ is the neutral element and

$$a \oplus b \oplus f(a,b) = e \tag{1}$$

for all $a, b \in X$. For the following exercise parts, you can assume this fact without proof.

e) Use (1) to express $a \oplus b$ using the function f and show that the map $X \times X \to X, (a, b) \mapsto a \oplus b$ is a morphism.

f) Show that $f(a, b) = f(b, a)$ and conclude that the group $(X, \oplus, e)$ is abelian.

This is an example of the *group law on an elliptic curve*. The analogous construction over finite fields is used in elliptic-curve cryptography.