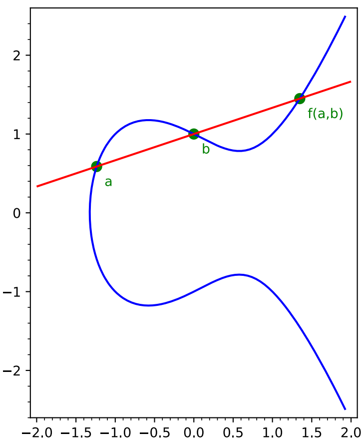
Presence Sheet 6

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.

Solution.

a) To find the projective closure, we homogenize the equation $g = x_2^2 - x_1^3 + x_1 - 1$ of x^0, finding

$$g^h = x_0 x_2^2 - x_1^3 + x_0^2 x_1 - x_0^3 \,.$$

Intersecting with the line $V(x_0)$ at infinity, we obtain

$$X \setminus X^0 = V(g^h, x_0) = V(-x_1^3, x_0) = \{(0:0:1)\}\,.$$

b) As seen in the lecture, the line L_{ab} is given by

$$L_{ab} = \{sa + tb : (s:t) \in \mathbb{P}^1_{\mathbb{C}}\} \subseteq \mathbb{P}^2_{\mathbb{C}}\,,$$

where for simplicity we choose some representatives $a, b \in \mathbb{C}^3$ of the points in $\mathbb{P}^2$. To obtain the third solution point $f(a,b)$, we calculate $g^h(sa+tb)$, note that it vanishes for $s = 0$ or $t = 0$ (since $a, b \in X$) and compute the third point $(s_0 : t_0)$ for which it vanishes. Then $f(a,b) = s_0 a + t_0 b$.

i) For the first set of points we have

$$sa + tb = (s + t : -s : s + t)$$

Plugging into g^h we obtain

$$\begin{aligned} g^h(sa+tb) &= (s+t)\cdot(s+t)^2 - (-s)^3 + (s+t)^2\cdot(-s) - (s+t)^3 \\ &= s^3 - s(s+t)^2 = s(s^2 - s^2 - 2st - t^2) = -st(t+2s)\,. \end{aligned}$$

So the third solution apart from $s = 0$ and $t = 0$ is $t = -2s$, leading to the point $sa + tb = s(a - 2b) = s(-1,-1,-1)$ and thus $f(a,b) = (-1:-1:-1) = (1:1:1)$.

ii) We have $sa + tb = (s : 0 : s+t)$ and plugging into f^h we obtain

$$g^h(sa+tb) = s(s+t)^2 - s^3 = s(s^2 + 2st + t^2 - s^2) = st(2s+t)$$

and so the third solution is (again) given by $t = -2s$, leading to $sa + tb = s(1, 0, -1)$ and so $f(a,b) = (1:0:-1)$.

c) As seen in class, the projective variety X is a variety and so $\Delta_X = X \times X \setminus U$ is closed in $X \times X$, hence U is open.

d) Similar to part b) we note that $g^h(sa+tb)$ is a homogeneous polynomial of degree 3 in the variables sa_i, tb_i for $i = 0,1,2$. The assumption $a, b \in X$ implies $g^h(a) =$

$g^h(b) = 0$, so that this polynomial vanishes when substituting $s = 0$ or $t = 0$. Thus separating out the variables s, t we have

$$g^h(sa + tb) = t^3 \underbrace{g_0(a, b)}_{=0 \text{ since } g^h|_{s=0}=0} + st^2 g_1(a, b) + s^2 t g_2(a, b) + s^3 \underbrace{g_3(a, b)}_{=0 \text{ since } g^h|_{t=0}=0},$$

where g_1 is bihomogeneous of degree 1 in a and 2 in b, and g_2 is bihomogeneous of degree $(2, 1)$. From this we see that the third solution $(s_0 : t_0)$ is given by $(s_0 : t_0) = (g_1(a, b) : -g_2(a, b))$ leading to the point

$$f(a, b) = g_1(a, b)a + g_2(a, b)b$$

This is again an expression which is homogeneous of degree 3 in both a, b, and thus it gives a morphisms at all points where it is defined. Since a, b are by definition linearly independent, the only possibility for it to be not well-defined is when $g_1(a, b) = g_2(a, b) = 0$, which would imply that g^h vanishes identically on the line L_{ab}. This is impossible since X is an irreducible curve of degree 3 and thus does not contain a line.

e) From the equation (1) we see that $a \oplus b$ is the additive inverse of $f(a, b)$. But given $c \in X$ we also have $e \oplus c \oplus f(e, c) = e$ which shows that $f(e, c)$ is the additive inverse of c. Substituting $c = f(a, b)$ we see

$$a \oplus b = f(e, f(a, b)) .$$

Since f is a morphisms, the map $(a, b) \mapsto a \oplus b$ is also a morphism as the composition

$$X \times X \xrightarrow{f} X \xrightarrow{(e, \mathrm{id}_X)} X \times X \xrightarrow{f} X ,$$

where $e : X \to X, c \mapsto e$ is the constant map.

f) By definition, for (a, b) with $a \neq b$ the point $f(a, b)$ is the third intersection point of the line L_{ab} with X. But $L_{ab} = L_{ba}$ and so $f(a, b) = f(b, a)$ for $(a, b) \in U$. But since $U \subseteq X \times X$ is non-empty and open, it is also dense (as X is irreducible) and so this equality also holds on all of X. Here we use that the two morphisms $X \times X \to X$ given by $(a, b) \mapsto f(a, b)$ and $(a, b) \mapsto f(b, a)$ agree on a closed set since X is a variety.

To conclude we just observe

$$a \oplus b = f(e, f(a, b)) = f(e, f(b, a)) = b \oplus a .$$