14. October 2015

# Exercise sheet 1<br>Elliptic Curves [1]

Kay Rülling

**Exercise 1.1.** Let $k$ be a field and $A$ a *local* $k$-algebra and write $\mathbb{P}^2_k = \operatorname{Proj} k[X,Y,Z]$. Show that the $A$-rational points over $k$ of $\mathbb{P}^2_k$ are given by

$$\mathbb{P}^2_k(A) = \{(a,b,c) \in A^3 \mid A = aA + bA + cA\}/\sim,$$

where $(a,b,c) \sim (a',b',c') :\Longleftrightarrow a = ua',\ b = ub',\ c = uc'$ for some unit $u \in A^\times$.

**Challenge:** Show that if $X$ is any $k$-scheme, then

$$\mathbb{P}^n_k(X) = \{\text{surjections of } \mathcal{O}_X\text{-modules } \mathcal{O}_X^{n+1} \xrightarrow{\varphi} \mathcal{L} \text{ with } \mathcal{L} \text{ invertible }\}/\sim,$$

where $\varphi \sim \varphi' \Longleftrightarrow$ there exists an isomorphism $\alpha : \mathcal{L} \xrightarrow{\simeq} \mathcal{L}'$ such that $\alpha \circ \varphi = \varphi'$.

**Exercise 1.2.** Let $k$ be a field and $A$ a local $k$-algebra.

(1) Let $F \in k[X,Y,Z]$ be a homogenous polynomial and set $C = \operatorname{Proj} k[X,Y,Z]/(F)$. Show

$$C(A) = \{(a:b:c) \in \mathbb{P}^2_k(A) \mid F(a,b,c) = 0\},$$

where we denote by $(a:b:c) \in \mathbb{P}^2_k(A)$, the image of $(a,b,c)$, with $aA + bA + cA = A$, in $\mathbb{P}^2_k(A)$ under the identification from Exercise 1.1.

(2) For $F \in k[X,Y,Z]$ homogeneous of degree $n$ define $f(x,y) \in k[x,y]$ by $f(\frac{X}{Z}, \frac{Y}{Z}) = \frac{1}{Z^n}F(X,Y,Z)$. Similar define $f_\infty(x) \in k[x]$ by $f_\infty(\frac{X}{Y}) = \frac{1}{Y^n}F(X,Y,0)$. Define $C$ as above. Show

$$C(k) =$$

$$\{(a,b) \in k^2 \mid f(a,b) = 0\} \sqcup \{a' \in k \mid f_\infty(a') = 0\} \sqcup \begin{cases} \emptyset & \text{if } F(X,0,0) = 0 \\ \{*\} & \text{else.} \end{cases}$$

[1] This exercise sheet will be discussed on October 21. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `l.zhang@fu-berlin.de`

**Exercise 1.3.** Set $f(x,y) = y^2 - x^3 + x \in \mathbb{Q}[x,y]$ and $U = \operatorname{Spec}\mathbb{Q}[x,y]/(f)$. In this exercise we want to show

$$U(\mathbb{Q}) = \{(0,0), (\pm 1, 0)\} \subset \mathbb{Q}^2.$$

For this proceed as follows: For $a \in \mathbb{Q}\setminus\{0\}$ define its height by $H(a) = \max\{|m|, |n|\}$, where $m, n \in \mathbb{Z}\setminus\{0\}$ with $a = m/n$ and $(m,n) = 1$; set $H(0) = 1$. Now we assume $S := U(\mathbb{Q}) \setminus \{(0,0), (\pm 1, 0)\}$is not empty. Choose a point $(x_0, y_0) \in S$ with $H(x_0)$ minimal. The aim is to construct a point $(x_1, y_1) \in S$ with $H(x_1) < H(x_0)$ therefore leading to a contradiction:

(1) Show that we can assume $x_0 > 1$. (*Hint:* If $(a,b) \in U(\mathbb{Q}) \setminus \{(0,0)\}$, then also $(-\frac{1}{a}, \frac{b}{a^2}) \in U(\mathbb{Q})$.)
(2) By 1 we can write $x_0 = m/n$ with natural numbers $m > n > 0$. Show that either $m$ or $n$ is even. (*Hint:* Else $(\frac{x_0+1}{x_0-1}, \frac{2y_0}{(x_0-1)^2}) \in S$ and $H(\frac{x_0+1}{x_0-1}) < H(x_0)$.)
(3) Use the above and $(x_0-1)x_0(x_0+1) = y_0^2$ to show that $x_0$ and $x_0 \pm 1$ are squares of rational numbers.
(4) Set
$$T := \{(c,d,e) \in \mathbb{Q}^3 \mid c^2 + 1 = d^2 = e^2 - 1\}.$$
Then there are mutually inverse maps $f : T \to S$ and $g : S \to T$ given by
$$f(c,d,e) = (c^2 + 1 + cd + ce + de, (c+d)(c+e)(d+e))$$
and
$$g(a,b) = (\frac{1}{2b}((a-1)^2 - 2), \frac{1}{2b}(a^2+1), \frac{1}{2b}((a+1)^2 - 2)).$$
(5) There is a map $h : T \to U(\mathbb{Q})$ given by $h(c,d,e) = (c^2+1, cde)$.
(6) The composition $h \circ g : S \to U(\mathbb{Q})$ has image $\{(a,b) \in U(\mathbb{Q}) \mid a, a \pm 1 \text{ are squares in } \mathbb{Q}\}$.
(7) Putting 3 and 6 together show that there exists $(x_1, y_1) \in S$ with $h(g(x_1, y_1)) = (x_0, y_0)$.
(8) Show that $H(x_1) < H(x_0)$. This yields a contradiction.

**Remark 1.** The map $h \circ g : S \to U(\mathbb{Q})$ is induced from the multiplication-with-2 map on the elliptic curve defined by $f$.

**Exercise 1.4.** Let $E \subset \mathbb{P}^2_{\mathbb{Q}}$ be the elliptic curve given by $y^2 = x^3 - x$ (i.e. $E = \operatorname{Proj}\mathbb{Q}[X,Y,Z]/(ZY^2 - X^3 + Z^2X)$). Given two points $P, Q \in E(\mathbb{Q})$ there is a unique line $L = V_+(aX + bY + cZ)$, $a, b, c \in \mathbb{Q}$, passing through this points (if $P = Q$ take $L$ to be the tangent line) and $L(\mathbb{Q})$ intersects $E(\mathbb{Q})$ in a third point $R_0$. (This is a bit imprecise, since it can happen for example that $R$ is equal to $P$. It is part of the exercise to make this more precise.) Then there is a unique line $L_1$ passing through $R_0$ and the point at infinity (given by the prime ideal $(X, Z)$) which intersects $E(\mathbb{Q})$ in a third point $R$. Show that $E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$, $(P, Q) \mapsto P + Q := R$ defines a group structure on $E(\mathbb{Q})$ so that $E(\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$. Which point of $E(\mathbb{Q})$ is the neutral element? (*Hint:* Use Exercise 1.3.)