18. November 2015

Exercise sheet 6
Elliptic Curves [1]

Kay Rülling

Exercise 6.1. Let k be a field of characteristic $\neq 2, 3$ and $E \subset \mathbb{P}^2_k$ an elliptic curve given by

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in k, 4a^3 + 27b^2 \neq 0.$$

Hence

$$E(k) = \{(x, y) \in k^2 \mid y^2 = x^3 + ax + b\} \cup \{O\},$$

where O corresponds to the point $Z = 0, X = 0$. Recall that the group structure on $E(k)$ is defined such that the injective map

$$E(k) \to \mathrm{Pic}^0(E) \to \mathrm{CH}^1(E), \quad P \mapsto \mathcal{O}_E([P] - [O]) \mapsto [P] - [O]$$

is a group homomorphism. We denote by $+_E$ the group law on $E(k)$.

(1) Let $P, Q, S \in E(k)$. Show that $P +_E Q = S$ if and only if there exists a function $f \in k(E)^\times$ such that $\mathrm{div}(f) = [P] + [Q] - [S] - [O]$.

Fix two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $E(k) \setminus \{O\}$ and assume $x_1 \neq x_2$.

(2) Show that there is a unique line $L_1 = V_+(c_1X + d_1Y + e_1Z) \subset \mathbb{P}^2_k$, such that $L_1(k) \cap E(k) = \{P, Q, R\}$ for some point $R \in E(k)$.
(3) Show that there is a unique line $L_2 = V_+(c_2X + d_2Y + e_2Z) \subset \mathbb{P}^2_K$ such that $L_2(k) \cap E(k) = \{R, O, S\}$, for some point $S \in E(k) \setminus \{O\}$.
(4) Show that $P +_E Q = S$. (*Hint:* Denote by $f \in k(E)$ the image of $\frac{c_1X + d_1Y + e_1Z}{c_2X + d_2Y + e_2Z}$ and compute $\mathrm{div}(f)$.)
(5) Show that S is equal to (x, y) with

$$x = \frac{x_1x_2^2 + x_1^2x_2 - 2y_1y_2 + a(x_1 + x_2) + 2b}{(x_1 - x_2)^2}, \quad y = \frac{W_2y_2 - W_1y_1}{(x_1 - x_2)^3},$$

where

$$W_1 = 3x_1x_2^2 + x_2^3 + a(x_1 + 3x_2) + 4b, \quad W_2 = 3x_1^2x_2 + x_1^3 + a(3x_1 + x_2) + 4b.$$

[1] This exercise sheet will be discussed on November 24. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `l.zhang@fu-berlin.de`

Exercise 6.2. Let C be a smooth projective curve over a field k and assume $C(k) \neq \emptyset$. Let $L = \mathcal{O}_C(\sum_i n_i[P_i])$ be a line bundle on C and recall that its degree (over k) is equal to $\deg_k(L) = \sum_i n_i \cdot [k(P_i) : k]$. Also recall that if C' is a smooth projective curve and $f : C' \to C$ is a finite surjective morphism, then we defined the pullback

$$f^*(\sum_i n_i[P_i]) := \sum_i n_i \sum_{Q \in f^{-1}(P_i)} e(Q/P_i)[Q],$$

where the $e(Q/P_i)$ are the ramification indices.

(1) Let $f : C' \to C$ be as above and $L = \mathcal{O}_C(D)$ a line bundle on C given by the divisor D. Show that $f^*L = \mathcal{O}_{C'}(f^*D)$.

(2) Let K/k be a finitely generated field extension. Denote by $C_K = C \times_{\operatorname{Spec} k} \operatorname{Spec} K$ the base change and by $\pi : C_K \to C$ the projection. Show that $\deg_K(\pi^*L) = \deg_k(L)$. (*Hint:* Consider the cases where K/k is finite and purely transcendental, separately. In the case where K/k is finite show that $[K : k] \cdot \deg_K(\pi^*L) = [K : k] \cdot \deg_k(Ł)$ using the $\sum_i e_i f_i = n$ formula.)

(3) Let $f : S \to T$ be a morphism of k-schemes. Show that $(\mathrm{id}_C \times f)^* : \operatorname{Pic}(C \times T) \to \operatorname{Pic}(C \times S)$ sends $\operatorname{Pic}^0(C \times T)$ to $\operatorname{Pic}^0(C \times S)$.

Exercise 6.3. Let k be a field.

(1) Let X, Y be k-schemes and denote by $p_1 : X \times Y \to X$ the projection. We have a natural map $\Omega^1_{X/k} \to p_{1*}\Omega^1_{X \times_k Y/Y}$. Show the natural map induced by adjunction $p_1^*\Omega^1_{X/k} \to \Omega^1_{X \times_k Y/Y}$ is an isomorphism. (*Hint:* It suffices to check this locally, hence to show $B \otimes_k \Omega^1_{A/k} \cong \Omega^1_{A \otimes_k B/B}$. This follows easily from the universal property.)

(2) Let G be a group scheme over k. Denote by $\pi : G \to \operatorname{Spec} k$ the structure map, by $m : G \times_k G \to G$ the group law, by $\iota : G \to G$ the inverse and by $e : \operatorname{Spec} k \to G$ the neutral section (see Exercise sheet 4.) Consider $G \times_k G$ as a G-scheme via the second projection p_2. Show that $\tau = m \times p_2 : G \times_k G \to G \times_k G$ is an automorphism of G-schemes.

(3) Show that $m^*\Omega^1_{G/k} \cong p_1^*\Omega^1_{G/k}$. (*Hint:* From (2) we get an isomorphism $\tau^*\Omega^1_{G \times G/G} \cong \Omega^1_{G \times G/G}$. Then use (1).)

(4) Show that $\Omega^1_{G/k} \cong \pi^* e^* \Omega^1_{G/k}$. (*Hint:* Pullback (3) along $\mathrm{id} \times \iota : G \to G \times_k G$.)

Exercise 6.4. Let C be a smooth projective curve over a field k which has the structure of a group scheme. Show that C is an elliptic curve. (*Hint:* Use Exercise 6.3, (4) to show that ω_C is trivial and conclude.)