2. December 2015

Exercise sheet 7
Elliptic Curves [1]

Kay Rülling

Exercise 7.1. Which of the following Weierstraß equations over $\mathbb{Q}$ are smooth (and hence define elliptic curves)? Are some of them isomorphic over $\mathbb{Q}$? In the smooth cases when viewing it as an elliptic curve over $\mathbb{Q}_5$ find a minimal Weierstraß equation and say whether it has good reduction.

(1) $y^2 = x^3$
(2) $y^2 = x^3 + x$
(3) $y^2 = x^3 + 1$
(4) $y^2 = x^3 + 5x + 7$
(5) $y^2 = x^3 + 20x + 56$
(6) $y^2 = x^3 + 625x$

Exercise 7.2. Consider the Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 + 22x - 9.$$

Show that its discriminant is $\Delta = -2^{15} \cdot 5^2$ and $c_4 = -5 \cdot 211$. Show that if we view it as an Weierstraß equation over $\mathbb{Q}_p$, then it is minimal, where p is any prime.

Exercise 7.3. Let A be a DVR with residue field k and fraction field K. Set $S = \operatorname{Spec} A$ and denote by $s = \operatorname{Spec} k$ and $\eta = \operatorname{Spec} K$, the closed and generic point of S, respectively. Let $\pi : \mathcal{C} \to S$ be a surjective morphism from an integral scheme $\mathcal{C}$, such that its generic fiber $C_\eta = C \times_S \eta \to \eta$ and its special fiber $C_s = C \times_S s \to s$ are smooth of relative dimension 1. Let $\sigma : S \to \mathcal{C}$ be a closed immersion over S, i.e. a section of π. Show that its ideal sheaf $\mathcal{I}$ is invertible.

(*Hint:* It suffices to check that the stalks in the points $\sigma(\eta)$ and $\sigma(s)$ are free of rank 1. $\mathcal{I}_{\sigma(\eta)}$ is the ideal sheaf of $\sigma(\eta) \hookrightarrow C_\eta$ and hence is invertible, since C_η is smooth. For $\mathcal{I}_{\sigma(s)}$ it suffices to check

[1] This exercise sheet will be discussed on December 9 and 16. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `l.zhang@fu-berlin.de`

that $\mathcal{I}_{\sigma(s)} \otimes_{\mathcal{O}_{\mathcal{C},\sigma(s)}} k(\sigma(s))$ is $k(s)$-vector space of dimension 1 (see Exercise 5.2, (1)). To this end show that this vector space is equal to $\mathcal{O}_{\mathcal{C}_s}(-[\sigma(s)])_{\sigma(s)} \otimes_{\mathcal{O}_{\mathcal{C}_s,\sigma(s)}} k(s)$ to conclude. For the latter use that the sequence $0 \to \mathcal{I}_{\sigma(s)} \to \mathcal{O}_{\mathcal{C},\sigma(s)} \to A \to 0$ is split exact and hence stays exact when pulled back to the special fiber.)

Exercise 7.4. Let K be a complete discrete valuation field with ring of integers equal to A and residue field k. Set $S = \operatorname{Spec} A$ and denote by η and s the generic and the closed point of S, respectively. Let E/K be an elliptic and $P_0 \in E(K)$ a fixed K-rational point. We assume E/K has good reduction and denote by $\bar{E}/k$ its reduction, i.e. we take a minimal Weierstraß equation for E/K which defines a model $\mathcal{W}/A$ and the following commutative diagram in which both squares are cartesian

$$\begin{tikzcd} E \arrow[r, "j"] \arrow[d] & \mathcal{W} \arrow[d] & \bar{E} \arrow[l, "i"'] \arrow[d] \\ \eta \arrow[r] & S & s. \arrow[l] \end{tikzcd}$$

We denote by

$$\sigma : E(K) \to \bar{E}(k)$$

the reduction map which we defined in the lecture.

(1) Let $\tilde{P} = (a : b : c) \in \mathcal{W}(A) \subset \mathbb{P}^2(A)$ be an A-rational point (see Exercise 1.1 for notation). It defines a closed subscheme of $\mathcal{W}$ and we denote by $\mathcal{O}_{\mathcal{W}}(-[\tilde{P}])$ the corresponding ideal sheaf. Show that $\mathcal{O}_{\mathcal{W}}(-[\tilde{P}])$ is invertible. (*Hint:* Exercise 7.3.)

(2) Let $\tilde{P}$ be as above. Denote by $P \in E(K)$ its inverse image along j and by $\bar{P}$ its inverse image along i. Show

$$j^*\mathcal{O}_{\mathcal{W}}(-[\tilde{P}]) = \mathcal{O}_E(-[P]), \quad i^*\mathcal{O}_{\mathcal{W}}(-[\tilde{P}]) = \mathcal{O}_{\bar{E}}(-[\bar{P}]),$$

where the right hand sides are the usual invertible sheaves which we defined on smooth curves.

(3) Denote by $\operatorname{Pic}^0(\mathcal{W})$ the subgroup of $\operatorname{Pic}(\mathcal{W})$ consisting of line bundles L on $\mathcal{W}$ such that $\deg_K(j^*L) = 0$ and $\deg_k(i^*L) = 0$. Show that $j^* : \operatorname{Pic}^0(\mathcal{W}) \to \operatorname{Pic}^0(E)$ is surjective. (*Hint:* By the isomorphism $E(K) \cong \operatorname{Pic}^0(E)$ any line bundle $L \in \operatorname{Pic}^0(E)$ can be represented by a line bundle of the form $\mathcal{O}_E([P] - [P_0])$. Use this and 1, 2.)

(4) Show that $j^* : \operatorname{Pic}^0(\mathcal{W}) \to \operatorname{Pic}^0(E)$ is also injective and hence is an isomorphism.

(5) Show that the following diagram commutes

$$\begin{tikzcd} & \mathrm{Pic}^0(\mathcal{W}) \arrow[dl, "j^*\simeq"'] \arrow[dr, "i^*"] & \\ \mathrm{Pic}^0(E) \arrow[d, "\simeq"] & & \mathrm{Pic}^0(\bar{E}) \arrow[d, "\simeq"] \\ E(K) \arrow[rr, "\sigma"] & & E(k). \end{tikzcd}$$

(6) Conclude that σ is a group homomorphism.

Exercise 7.5. Let k be an algebraically closed field of characteristic $\neq 2$. Let E/k be an elliptic curve. Show that it has a Weierstraß equation of the form

$$y^2 = x(x-1)(x-\lambda), \quad \lambda \in k \setminus \{0,1\}.$$

This is called a Legendre equation for E. (*Hint:* Since we are in characteristic $\neq 2$ we find a Weierstraß equation of the form $y^2 = x^3 + ax^2 + bx + c$. Since k is algebraically closed we can factor the polynomial on the right of the equality as $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, $\alpha_i \in k$. Then show that the discriminant is given by $\Delta = 16(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$. Since $\Delta \neq 0$ one can define $\lambda = \frac{\alpha_3-\alpha_1}{\alpha_2-\alpha_1}$. Show that the Legendre form can be achieved with this particular λ.)

Exercise 7.6. Let k be a field with algebraic closure $\bar{k}$. Show that for any $j_0 \in \bar{k}$ there exists an elliptic curve $E/k(j_0)$ with j-invariant $j(E) = j_0$. Concretely, show

(1) If $j_0 \neq 0, 1728$, then the Weierstraß equation

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

has $\Delta = \frac{j_0^3}{(j_0-1728)^3}$ and $j = j_0$.

(2) The Weierstraß equation $y^2 + y = x^3$ has $\Delta = -27$ and $j = 0$.

(3) The Weierstraß equation $y^2 = x^3 + x$ has $\Delta = -64$ and $j = 1728$.

The following two exercise are equal to the Exercises 6.3 and 6.4.

Exercise 7.7. 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 7.8. 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 7.7, (4) to show that ω_C is trivial and conclude.)