11. November 2015

Exercise sheet 5
Elliptic Curves [1]

Kay Rülling

Recall: A finite field extension L/k is called *separable* if for any element $a \in L$, its the minimal polynomial $f_a \in k[x]$ has no multiple roots in an algebraic closure, equivalently f_a and f'_a(= its formal derivation) are coprime. A finitely generated field extension K/k is called separable if there is a purely transcendental extension $k(t_1, \dots, t_r)/k$ inside of K such that $K/k(t_1, \dots, t_r)$ is finite separable. If k is a perfect field, then any finitely generated field extension K/k is separable.

Exercise 5.1. (1) Let $K = k(t_1, \dots, t_r)/k$ be a transcendental field extension. Show that $\Omega^1_{K/k}$ is a free $k(t_1, \dots, t_r)$-vector space of dimension r. (*Hint:* $\Omega^1_{K/k} = \Omega^1_{k[t_1,\dots,t_r]/k} \otimes_{k[t_1,\dots,t_r]} K$.)

(2) Let K/k be a field extension and L/K finite separable. Show that the natural map $\Omega^1_{K/k} \otimes_K L \to \Omega^1_{L/k}$ is an isomorphism. (*Hint:* Write $L \cong K[x]/(f)$ and use the exact sequence of L-vector spaces $(f)/(f)^2 \to \Omega^1_{K[x]/k} \otimes_{K[x]} L \to \Omega^1_{L/k} \to 0$, in which the first map sends the class of f to df.)

(3) Let L/K be a purely inseparable field extension of degree p, i.e. $L \cong K[X]/(X^p - a)$, where $a \in K \setminus K^p$. Show that there is an isomorphism

$$\left(\frac{\Omega^1_{K/k}}{K \cdot da} \otimes_K L\right) \oplus L da \xrightarrow{\simeq} \Omega^1_{L/k}, \quad (\alpha, a_1 da) \mapsto \alpha + a_1 da.$$

(4) Let K/k be a finitely generated field extension of transcendence degree r. Conclude from the above that K/k is separable if and only if $\dim_K \Omega^1_{K/k} = r$.

Exercise 5.2. (1) Let A be a noetherian integral local ring with residue field k and fraction field K and M a finitely generated A-module. Show that if $\dim_k(M \otimes_A k) = \dim_K(M \otimes_A K) = r$, then M is a free A-module of rank r. (*Hint:* By Nakayama's Lemma M is generated by r elements.)

[1]This exercise sheet will be discussed on November 17. If you have questions or remarks please contact `kay.ruelling@fu-berlin.de` or `l.zhang@fu-berlin.de`

(2) Let $A = k[x_1, \dots, x_n]/I$, where $I = (f_1, \dots, f_r)$. Assume k is algebraically closed and A is integral and has Krull dimension $\dim A = d$. Denote by $J = (\partial f_i/\partial x_j)$ the Jacobian matrix; it is an $n \times r$-matrix with coefficients in $k[x_1, \dots, x_n]$. Assume that for all $\underline{a} \in k^n$ with $f_i(\underline{a}) = 0$, all i, the rank of $J(\underline{a})$ is $n - d$. Show that $\Omega^1_{A/k}$ is a locally free A-module of rank d. (*Hint:* $\underline{a}$ as above defines a map $A \to k(\underline{a}) = k$. Show that $\Omega^1_{A/k} \otimes_A k(\underline{a})$ has vector space dimension d. To this end use the exact sequence of A-modules $I/I^2 \to \Omega^1_{k[x_1,\dots,x_n]/k} \otimes_{k[x_1,\dots,x_n]} A \to \Omega^1_{A/k} \to 0$, in which the first map sends the class of f_i to df_i. Then conclude with Exercise 5.1 and (1).)

(3) Let k be a field and X a smooth integral k-scheme of dimension d. Show that $\Omega^1_{X/k}$ is locally free of rank d.

Exercise 5.3. Let k be a field of characteristic $\neq 2, 3$. Let $a, b \in k$ and set $E = \operatorname{Proj} k[X, Y, Z]/(Y^2 Z - (X^3 + aXZ^2 + bZ^3))$.

(1) Set $U = \operatorname{Spec} k[x, y]/(y^2 - (x^3 + ax + b))$, where $x = X/Z, y = Y/Z$ and $W = \operatorname{Spec} k[u, z]/(z - (u^3 + auz^2 + bz^3))$, where $u = X/Y$, $z = Z/Y$. Show that $U, W \subset E$ are open and $E = U \cup W$.

(2) Show that E is a smooth k-scheme if and only if $4a^3 + 27b^2 \neq 0$.

We assume $4a^3 + 27b^2 \neq 0$ in the following.

(3) Show that E is an elliptic curve.

(4) Set $U_1 = U \setminus V(y)$, $U_2 = U \setminus V(3x^2 + a)$ and $U_3 = W \setminus V(1 - 2auz - 3bz^2)$. Show that $E = U_1 \cup U_2 \cup U_3$ is an open covering.

(5) Define the differential forms

$$\alpha_1 := \frac{dx}{2y} \in \Gamma(U_1, \omega_E), \quad \alpha_2 := \frac{dy}{3x^2 + a} \in \Gamma(U_2, \omega_E),$$

$$\alpha_3 := -\frac{du}{1 - 2auz - 3bz^2} \in \Gamma(U_3, \omega_E),$$

where $\omega_E := \Omega^1_{E/k}$. Show that there is a differential $\alpha \in \Gamma(E, \omega_E)$ with $\alpha_{|U_i} = \alpha_i$, $i = 1, 2, 3$.

(6) Show that we have an isomorphism $\mathcal{O}_E \to \omega_E$, $f \mapsto f \cdot \alpha$. (*Hint:* We know from the lecture that $\omega_E \cong \mathcal{O}_E$ abstractly.)