Exercise Sheet 8

Discussed on 16.06.2021

Problem 1. Let $R = \varinjlim_{i \in I} R_i$ be a filtered colimit of rings.[1]

(a) Let $X \to \operatorname{Spec} R$ be a morphism of schemes which is of finite representation. Show that there is some $i \in I$ and a scheme X_i over $\operatorname{Spec} R_i$ such that $X = X_i \times_{\operatorname{Spec} R_i} \operatorname{Spec} R$.

(b) Fix some element $0 \in I$ and let $X_0, Y_0 \to \operatorname{Spec} R_0$ be morphisms of schemes which are of finite presentation. For every $i \geq 0$ let X_i and Y_i denote the base-change to $\operatorname{Spec} R_i$, and let X and Y denote the base-change to $\operatorname{Spec} R$. Show that

$$\operatorname{Hom}_R(X, Y) = \varinjlim_i \operatorname{Hom}_{R_i}(X_i, Y_i)$$

(c) Let k be a field and let E and E' be two elliptic curves over k. Deduce from (b) that there is some finite field extension k'/k such that

$$\operatorname{Hom}(E_{k'}, E'_{k'}) = \operatorname{Hom}(E_{\overline{k}}, E'_{\overline{k}}),$$

where $\overline{k}$ denotes an algebraic closure of k. Here Hom denotes homomorphisms of elliptic curves (over their respective field).

Problem 2. Let k be an algebraically closed field and let K/k be any field extension.

(a) Convince yourself that $\operatorname{Hom}_k(\mathbb{P}^1_k, \mathbb{P}^1_k)$ is "much larger" than $\operatorname{Hom}_K(\mathbb{P}^1_K, \mathbb{P}^1_K)$ if $K \neq k$.

(b) Let E and E' be elliptic curves over k. Show that

$$\operatorname{Hom}(E, E') = \operatorname{Hom}(E_K, E'_K).$$

Hint: Pick any $\varphi \colon E_K \to E'_K$ on the right-hand side. Using problem 1, show that there is a finite-type k-algebra $R \subset K$ such that φ comes via pullback from a homomorphism $\psi \colon E_R \to E'_R$. Pick a closed point $x \in \operatorname{Spec} R$. It is k-rational and hence induces a homomorphism $\psi_0 \colon E_R \to E'_R$ coming via base-change from a morphism $E \to E'$. Using the rigidity lemma from lecture 6, show that $\psi - \psi_0 = 0$.

[1] If you are not comfortable with filtered colimits, you can without loss of generality assume that all R_i are subrings of R. In this case we have $R = \bigcup_i R_i$ and for any $i, j \in I$ there is some $k \in I$ such that $R_i \subset R_k$ and $R_j \subset R_k$.

Problem 3. Let L be a number field (i.e. a finite extension of $\mathbb{Q}$) and let E be an elliptic curve over L. Let $\mathcal{O}_L \subset L$ be the ring of integers.[2]

(a) Show that there is an integer $d \in \mathbb{Z}$ and an elliptic curve E' over $\mathcal{O}_L[d^{-1}]$ such that $E'_L \cong E$.

(b) Show that there is some integer e with

$$\mathrm{End}(E) = \mathrm{End}(\mathcal{O}_L[(de)^{-1}] \otimes_{\mathcal{O}_L} E').$$

(c) Assume that E admits complex multiplication by $\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers in some quadratic extension K over $\mathbb{Q}$. Let $p \in \mathbb{Z}$ be a prime not dividing de and let $\mathfrak{p} \subset \mathcal{O}_L$ be any prime ideal over p. Let $E'_{\mathfrak{p}}$ be the reduction of E' at $\mathfrak{p}$ (i.e. the base-change to $\mathcal{O}_L/\mathfrak{p}$). Then $E'_{\mathfrak{p}}$ is ordinary (resp. supersingular) if and only if p is split (resp. non-split) in K.

[2]For this problem all you need to know about $\mathcal{O}_L$ is that $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Q} = L$, i.e. L is obtained from $\mathcal{O}_L$ by inverting all integers.