Elliptic curves: exercise sheet 11

Due: 3rd December 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 31. Let $m > 0$ be an integer. Let F be a field of characteristic not dividing m, and suppose that F contains the group μ_m of m-th roots of unity. Let $A \subset F^*$ be a subgroup for which $A/(A \cap F^{*m})$ is finite. Let $K = F(\sqrt[m]{a} : a \in A)$.

(a) Show that K is a finite Galois extension of F. Put $G = \mathrm{Gal}(K/F)$.

(b) Show that the map $A/(A \cap F^{*m}) \longrightarrow \mathrm{Hom}(G, \mu_m)$ given by $a \mapsto f_a$ where $f_a(\sigma) = \sigma(\sqrt[m]{a})/\sqrt[m]{a}$ for all $\sigma \in G$, is a well defined injective group homomorphism.

(c) Show that the map $G \longrightarrow \mathrm{Hom}(A/(A \cap F^{*m}), \mu_m)$ given by $\sigma \mapsto g_\sigma$ where $g_\sigma(a) = \sigma(\sqrt[m]{a})/\sqrt[m]{a}$ is a well defined injective group homomorphism.

Exercise 32. Let $m > 0$ be an integer. Let E be an elliptic curve over a field F of characteristic not dividing m. Suppose that the m-torsion points of E are defined over F. Let $E[m]$ denote the group of m-torsion points of E and let $A \subset E(F)$ be a subgroup for which $A/(A \cap mE(F))$ is finite. For any $P \in E(F)$, we let $\frac{1}{m}P$ denote a point $Q \in E(\overline{F})$ for which $mQ = P$. Let K be the extension of F generated by the coordinates of the points $\frac{1}{m}P \in E(\overline{F})$ for which $P \in A$.

(a) Show that K is a finite Galois extension of F. Show that it does not depend on the choices of the points $\frac{1}{m}P$. Put $G = \mathrm{Gal}(K/F)$.

(b) Show that the map $A/(A \cap mE(F)) \longrightarrow \mathrm{Hom}(G, E[m])$ given by $P \mapsto f_P$ where $f_P(\sigma) = \sigma(\frac{1}{m}P) - \frac{1}{m}P$ for all $\sigma \in G$, is a well defined injective group homomorphism.

(c) Show that the map $G \longrightarrow \mathrm{Hom}(A/(A \cap mE(F)), E[m])$ given by $\sigma \mapsto g_\sigma$ where $g_\sigma(a) = \sigma(\frac{1}{m}P) - \frac{1}{m}P$ is a well defined injective group homomorphism.

Exercise 33. Let $x, y \in \mathbf{Q}$. Let $P = (1 : x)$ and $Q = (1 : y)$ in $\mathbf{P}_1(\mathbf{Q})$ and let $R = (1 : x + y : xy)$ in $\mathbf{P}_2(\mathbf{Q})$. Let h denote the height function on $\mathbf{P}_1(\mathbf{Q})$ and $\mathbf{P}_2(\mathbf{Q})$ respectively. Show that $|h(R) - h(P) - h(Q)|$ is bounded by $\log 2$.

Exercise 34. For every $B \in \mathbf{R}_{>0}$ let X_B denote the subset of points of $\mathbf{P}_1(\mathbf{Q})$ of height $\leq B$.

(a) Determine $\#X_B$ when $B = (\log m)$ for the integers $1 \leq m \leq 10$.

(b) Determine

$$\lim_{B \to \infty} \frac{\#X_B}{e^B}.$$

Exercise 35. Let E be the elliptic curve over $\mathbf{Q}$ given by $y^2 + y = x^3$.

(a) Let k be the number field generated by the 2-torsion points of E. Determine a finite set S of prime ideals of O_k for with the property that the reduction map $E(k)[2] \longrightarrow E(k_{\mathfrak{p}})$ is injective for every prime $\mathfrak{p} \notin S$.

(b) Same question, but for the 3-torsion points.

Exercise 36. Let E be an elliptic curve over $\mathbf{R}$. Show that $E(\mathbf{R})$ is isomorphic to the circle group $\{z \in \mathbf{C}^* : |z| = 1\}$ or $E(\mathbf{R})$ is the product of the circle group and a group of order 2.

Exercise 37. Let A be an abelian group and suppose that $h : A \longrightarrow \mathbf{R}_{\geq 0}$ is a function satisfying

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1), \qquad \text{for } P, Q \in A.$$

Here the O-symbol does not depend on P and Q, but only on A and h.

(a) Show that there is a constant $c \in \mathbf{R}$ such that $h(P) < c$ for all $P \in A$ of finite order.

(b) Show that

$$\langle P, Q \rangle = \frac{1}{2}(h(P + Q) - h(P) - h(Q))$$

is symmetric and almost bilinear and almost positive definite in the sense that $\langle P, P \rangle > c$ and $c' < \langle P + Q, R \rangle - \langle P, R \rangle - \langle Q, R \rangle < c''$ for certain constants $c, c', c'' \in \mathbf{R}$ that do not depend on $P, Q, R \in A$.

Exercise 38. Let F be a perfect field and let G_F denote the absolute Galois group of F. In other words $G_F = \mathrm{Gal}(\overline{F}/F)$. Let M be a G_F-module. A 1-*cocycle* with values in M is a map $G_F \longrightarrow M$ satisfying $f(\sigma\tau) = \sigma(f(\tau)) + f(\sigma)$ for all $\sigma, \tau \in G_F$. A 1-*coboundary* is a 1-cocycle of the form $\sigma \mapsto \sigma(m) - m$ for some fixed $m \in M$. The first *cohomology group* of G with values in M is the group of 1-cocycles modulo its subgroup of 1-coboundaries. It is denoted by $H^1(G_F, M)$.

(a) Check that 1-coboundaries are 1-cocycles. Check that 1-cocycles form a group with composition $(f + g)(\sigma) = f(\sigma) + g(\sigma)$ for all $\sigma \in G_F$ and that the 1-coboundaries from a subgroup.

(b) Let $m > 0$ be an integer and let E be an elliptic curve over F. Show that the map

$$\delta : E(F)/mE(F) \longrightarrow H^1(G_F, E[m])$$

given by $\delta(P) = f_P$ where $f_P(\sigma) = \sigma(Q) - Q$ is a well defined injective group homomorphism. Here Q is any point in $E(\overline{F})$ satisfying $mQ = P$.

(c) Show that $H^1(G_F, E[m])$ is finite when $F = \mathbf{R}$ or a finite field.

*(d) Show that $H^1(G_{\mathbf{Q}}, E[m])$ is infinite.