ALGEBRAIC CURVES
EXERCISE SHEET 12

Unless otherwise specified, k is an algebraically closed field.

Exercise 1.

We recall the setting of the Cayley-Bacharach theorem: $F_1, F_2 \subseteq \mathbb{P}^2_k$ are two plane projective cubics intersecting cubics intersecting in 9 pairwise distinct points $A_i \in \mathbb{P}^2_k,\ 1 \leq i \leq 9$ and G is another cubic containing $A_i,\ 1 \leq i \leq 8$. Show that no 6 points among $\{A_i,\ 1 \leq i \leq 8\}$ lie on a quadric, unless G is a linear combination of F_1, F_2.

Exercise 2.

Let $A_1, A_2, A_3, B_1, B_2, B_3$ be pairwise distinct points on an irreducible plane projective quadric $Q \subseteq \mathbb{P}^2_k$. For $(i,j) \in \{(1,2),\ (2,3),\ (3,1)\}$, denote by C_{ij} the intersection point of lines $\overline{A_iB_j}$ and $\overline{A_jB_i}$ (show that these lines intersect in exactly one point). Show that C_{12}, C_{23}, C_{31} are collinear. This result is known as Pascal's theorem.

Exercise 3.

Let (E, O) be an elliptic curve.

(1) Show that the addition defined in class has neutral element O and that any point $P \in E$ has a (unique) inverse $-P$ (you may assume associativity of $+$ to prove uniqueness of the inverse).
(2) Show that $+$ is commutative.

If we further assume that $+$ is associative, $(E, +, O)$ is an abelian group. Consider $O \neq O' \in E$ and $Q = \varphi(O, O')$. We define $\alpha : E \to E$ by $\alpha(P) = \varphi(Q, P)$.

(3) Show that for $P_1, P_2 \in (E, +, O)$, $P_1 + P_2 + \varphi(P_1, P_2) = \varphi(O, O)$.
(4) Show that $\alpha : (E, +, O) \to (E, +, O')$ is a group isomorphism.

Therefore, the group structure on E does not depend on the choice of O.

Exercise 4.

Let E, O be an elliptic curve. We say that an element x in an abelian group $(G, +)$ is p-torsion ($p \in \mathbb{Z}$) if $p \cdot x = \underbrace{x + \ldots + x}_{p \text{ times}} = 0$.

A simple point $P \in E$ with tangent line L is called a flex if $I(P, E \cap L) > 2$. We admit that, if $char(k) = 0$, any nonsingular cubic has 9 distinct flexes (see Fulton, Problem 5.23). Suppose $char(k) = 0$ and O is a flex.

(1) Show that flexes are exactly 3-torsion points of E and that they form a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
(2) Let $P \in E$. How many lines through P are tangent to E at some point $P \neq Q \in E$? (Hint: show that $P + 2Q = O$ and use exercise 5.)

Exercise 5.

Let (E, O) be an elliptic curve. Suppose $char(k) = 0$ and O is a flex (for the definition of flex, see exercise 4).

(1) Show that $P \in E$ is 2-torsion if, and only if, the tangent to E at P passes through O. (See exercise 4 for the definition of torsion points.)

We may assume that $E = Y^2Z - X(X - Z)(X - \lambda Z)$ and $O = [0 : 1 : 0] \in E$, where $\lambda \neq 0, 1$ (see Fulton, Problem 5.24).

(2) Find 2-torsion points of E. Draw a real picture. Show that 2-torsion points of E form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(3) Show that the endomorphism $P \mapsto 2P$ of E is surjective. (Hint: if $2P \neq O$, find an explicit expression for the coordinates of $2P$ depending on coordinates of P.)