November 23

Throughout, k is an algebraically closed field of characteristic different from 2 and 3.

Exercise 1.

Let F be an ellipitic curve with neutral element $O = (0 : 1 : 0)$.

(a) Show that P is a flex if and only if $P + P + P = O$.

(b) A line passes through two distinct flexes P and Q. Show that its third intersection with F is also a flex.

(c) Show that $P + P = O$ if and only if the tangent line to F at P passes through O.

Exercise 2.

Let $\lambda \in k \setminus \{0, 1\}$ and consider

$$F = y^2z - x(x - z)(x - \lambda z)$$

an elliptic curve with neutral element $O = (0 : 1 : 0)$.

(a) In the chart $z = 1$, show that the tangent at a point (x_0, y_0) passes through O exactly when $y_0 = 0$.

(b) Use Exercise 1(c) to find every point $P \in F(k)$ with $P + P = O$.

(c) 1. Describe the sum of any two distinct points in (b).

2. Describe the group formed by the points in (b).

Exercise 3.

Consider

$$E : y^2z = x^3 + 4xz^2, \qquad O = (0 : 1 : 0), \quad A = (0 : 0 : 1), \quad B = (2 : 4 : 1), \quad D = (2 : -4 : 1).$$

(a) Check that E is nonsingular and that A, B, D lie on E.

(b) Find the tangent to E at B and show that $B + B = A$.

(c) Show that $A + A = O$ and $B + A = D$. Deduce that $\{O, A, B, D\}$ is a cyclic subgroup of $E(k)$ of order 4.

Exercise 4.

Assume $\operatorname{char} k = 0$. Consider the elliptic curve

$$E : \ y^2z = x^3 - 43xz^2 + 166z^3, \qquad O = (0 : 1 : 0), \qquad P = (3 : 8 : 1).$$

(a) Find the tangent at P and use it to show that $2P = (-5 : -16 : 1)$.

(b) Check that $R = (11 : 32 : 1)$ lies on E and on the line through P and $2P$. Deduce that $3P = -R$.

(c) Show that the tangent at $2P$ passes through $-R$. Deduce that $4P = R$ and that P has order 7.

Exercise 5.

Let $k_0 \subseteq k$ be a subfield and let

$$E : y^2z = x^3 + Axz^2 + Bz^3, \qquad A, B \in k_0, \quad 4A^3 + 27B^2 \neq 0,$$

with neutral element $O = (0 : 1 : 0)$. Write $E(k_0)$ for the points whose homogeneous coordinates can be chosen in k_0.

(a) Let $P, Q \in E(k_0)$. Show that their joining line, or the tangent at P when $P = Q$, has an equation with coefficients in k_0.

(b) By substituting the line into the equation of E, show that $P \cdot Q \in E(k_0)$. Include the case where the line passes through O.

(c) Deduce that $E(k_0)$ is a subgroup of $E(k)$.

Exercise 6.

Let F be the elliptic curve from Exercise 2. Fix $Q_0 \in F(k)$ and put $P = Q_0 \cdot Q_0$.

(a) Show that the tangent at $Q \in F(k)$ has third intersection P if and only if $Q + Q = Q_0 + Q_0$.

(b) Deduce that the points Q with this property are precisely the points $Q_0 + T$ with $T + T = O$. Use Exercise 2 to count them.

(c) How many distinct lines through P are tangent to F at a point $Q \neq P$? Treat the cases where P is a flex and where it is not.

Exercise 7.

Consider the elliptic curve $F = y^2z - x^3 - z^3$ with neutral element $O = (0 : 1 : 0)$. Choose $\zeta \in k$ with $\zeta^3 = 1$ and $\zeta \neq 1$, and define

$$\psi(x : y : z) = (\zeta x : y : z).$$

(a) Verify that ψ preserves $F(k)$ and fixes O. Show that

$$\psi(P \cdot Q) = \psi(P) \cdot \psi(Q),$$

including when $P = Q$. Deduce that ψ is an automorphism of the group $F(k)$.

(b) Show that for every $P \in F(k)$,

$$P + \psi(P) + \psi^2(P) = O.$$

(c) Find the points of $F(k)$ fixed by ψ. Show that they form a cyclic subgroup of order 3.