Mastermath course "Elliptic curves" - exercise set 2

8. Let $k \geq 1$ be an integer that is not divisible by the cube of any prime number, and denote by $\phi : C_k(\mathbf{Q}) \to C_k(\mathbf{Q})$ the *porism map* on the rational points of the curve $C_k : X^3 + Y^3 = kZ^3$ that sends $P \in C_k(\mathbf{Q})$ to the "third" intersection point of C_k with the tangent line in P.
   a. Show that for a projective point $P = (x : y : z)$, we have
   $$\phi(P) = \left(x(x^3 + 2y^3) : -y(2x^3 + y^3) : z(x^3 - y^3)\right).$$
   b. Deduce that for an affine point $P = (x, y, 1) \in C_k(\mathbf{Q})$, the points in the sequence
   $$P, \phi(P), (\phi \circ \phi)(P), (\phi \circ \phi \circ \phi)(P), \ldots$$
   are pairwise different unless we have ($k = 1$ and $xy = 0$) or ($k = 2$ and $x = y = 1$). What happens in these special cases?

9. Let $G = \mathrm{GL}_3(K)$ be the group of invertible 3×3-matrices with coefficients from K.
   a. Show that the linear action of G on K^3 gives rise to a natural transitive left action of G on the points and the lines in projective plane $\mathbf{P}^2(K)$.
   b. Show that this leads to a natural right action of G on the set of smooth cubics in $\mathbf{P}^2(K)$.
   c. Find an element $g \in G$ that maps the porism curve $C_k : X^3 + Y^3 = kZ^3$ to a Weierstrass curve $Y^2Z = X^3 + AXZ^2 + BZ^3$, and compute A and B.

10. Let $\mathcal{C}$ be a plane cubic curve defined over K, i.e., given by a homogeneous cubic equation $F(X, Y, Z) = 0$ in $\mathbf{P}^2(K)$, with $F \in K[X, Y, Z]$. Suppose that $\mathcal{C}$ does not contain a line (over an algebraic closure $\overline{K}$).
   a. Show that a point $P \in \mathcal{C}(K)$ is singular if and only if every line through P intersects $\mathcal{C}$ in P with multiplicity at least 2.
   b. Deduce that $\mathcal{C}$ has at most one singular point defined over $\overline{K}$.
   *c. Is a singular point of $\mathcal{C}$ necessarily defined over K?

11. Let $\mathcal{C}$ be a curve in $\mathbf{P}^2(\mathbf{Q})$ defined by an irreducible homogeneous cubic polynomial $F \in \mathbf{Q}[X, Y, Z]$, and $P \in \mathcal{C}(\mathbf{Q})$ a point with the property that almost all lines through P with rational slope intersect $\mathcal{C}$ in a rational point different from P. Show that P is a singular point of $\mathcal{C}$.

12. Let G be the group from exercise 9, and write $\mathbf{P}^2(K) = \mathbf{A}^2(K) \cup \{Z = 0\}$ for the standard decomposition of the projective plane as an affine xy-plane together with a 'line at infinity'.
   a. Describe the subgroup $H \subset G$ of elements that respect this decomposition, and show that the *affine transformations* of $\mathbf{A}^2(K) = K^2$ induced by the elements of H are the maps $\mathbf{A}^2(K) \to \mathbf{A}^2(K)$ of the form

$$P \longmapsto A(P) + Q$$

   with $A \in \mathrm{GL}_2(K)$ and $Q \in K^2$.
   b. Show that the set $\mathrm{Aff}_2(K)$ of affine transformations of K^2 is a group that fits in a split exact sequence

$$0 \longmapsto K^2 \longrightarrow \mathrm{Aff}_2(K) \longrightarrow \mathrm{GL}_2(K) \longrightarrow 0.$$

13. A *conic* defined over K is a smooth curve $\mathcal{C}$ in $\mathbf{P}^2(K)$ arising as the zero set of a homogeneous polynomial $F \in K[X, Y, Z]$ of degree 2.
   a. Show that the conic $X^2 + Y^2 = Z^2$ defined over $\mathbf{Q}$ is isomorphic to the projective line $\mathbf{P}^1(\mathbf{Q})$ in the sense that there is an injective map

$$\begin{aligned} \mathbf{P}^1(\mathbf{Q}) &\longrightarrow \mathbf{P}^2(\mathbf{Q}) \\ (\lambda : \mu) &\longmapsto (p_0(\lambda, \mu), p_1(\lambda, \mu), p_2(\lambda, \mu)) \end{aligned}$$

   with image $\mathcal{C}(\mathbf{Q})$ that can be defined by homogeneous quadratic polynomials $p_i \in \mathbf{Q}[X, Y]$.
   b. Can you generalize this to arbitrary conics over $\mathbf{Q}$?

14. Let $\mathcal{C}$ be a curve in $\mathbf{P}^2(K)$ given as the zero set of $F \in K[X_1, X_2, X_3]$, and $P \in \mathcal{C}(K)$ a smooth point. We call the tangent line T_P to $\mathcal{C}$ in P an *inflectional tangent* if it intersects $\mathcal{C}$ in P with multiplicity ≥ 3.
   a. Suppose $\mathrm{char}(K) \neq 2$. Show that T_P is an inflectional tangent if and only if the determinant of the Hessian matrix

$$H(F) = \left(\partial^2 F / \partial X_i \partial X_j\right)_{i,j=0}^{2}$$

   vanishes in P.
   b. Compute the inflectional tangents to the curve $X^3 + Y^3 = Z^3$ that are defined over $K = \mathbf{Q}$, and over $K = \mathbf{C}$
   c. How many inflectional tangents does a smooth cubic curve have over $K = \mathbf{C}$?