Coursework 2 on chapter 4 and 5

1. Let $a \in \mathbb{Q}$ be some constant. Let $C : X^3 + Y^3 + Z^3 - a\,XYZ = 0$ be a cubic curve defined over $\mathbb{Q}$. Determine for which value of a is C smooth.

2. Let $C : X^3 - 2X^2Z + XY^2 - XZ^2 - 2Y^2Z + 2Z^3 = 0$ over $\mathbb{R}$. Determine if C is smooth.

3. Let C be a cubic curve defined over a field k with two singular points. Show that $C(k)$ contains $L(k)$ for some line L.

4. (a) Suppose P, Q and R are three distinct points in $\mathbb{P}^2$ that do not lie on one line. Prove that there is a change of variables $X' = a_1X + b_1Y + c_1Z$, $Y' = a_2X + b_2Y + c_2Z$ and $Z' = a_3X + b_3Y + c_3Z$ such that $P = (1 : 0 : 0)$, $Q = (0 : 1 : 0)$ and $R = (0 : 0 : 1)$ in the new coordinates. Explain how one finds the inverse change of variables.

   (b) Let $F \in k[X, Y, Z]$ be a homogeneous polynomial of degree d. Let $\ell(s : t)$ parametrise a line L. Suppose that $F\big(\ell(s : t)\big) = 0$ as a polynomial in $k[s, t]$. Show that the equation of the line L is a factor of the polynomial F. (We say that L is a component of the projective curve $C : F = 0$.)

5. Let C be a cubic curve with two distinct points O_1 and O_2. They can be used to defined to two groups: G_1 with the operation $\oplus_1$ on the elliptic curve (C, O_1) and G_2 with the operation $\oplus_2$ on the elliptic curve (C, O_2).

   a) Prove that $P \oplus_2 Q = (P \oplus_1 Q) \oplus_2 O_1$. In particular $P = (P \oplus_1 O_2) \oplus_2 O_1$.
   b) Consider the map $f : C \to C$ given by $f(P) = P \oplus_1 O_2$. Show that this is a group homomorphism $G_1 \to G_2$.
   c) Define an inverse map and use it to prove that G_1 and G_2 are isomorphic.

   Warning: Don't omit any () unless you are using associativity for one law only. E.g. $(P \oplus_1 Q) \oplus_2 R$ is not $P \oplus_1 (Q \oplus_2 R)$.

6. Let E be the elliptic curve defined by $y^2 = x^3 + 3$ over $\mathbb{F}_{13}$. Determine the group structure of $E(\mathbb{F}_{13})$.

7. Let E be an elliptic curve in Weierstrass form with A and B integer. Let $P = (x_P : y_P : 1)$ be a point in $E(\mathbb{Q})$. Write the rationals $x_P = \frac{a}{c}$ and $y_P = \frac{b}{d}$ as reduced fractions with $c, d > 0$.

   (a) Use
   $$b^2c^3 = (a^3 + A\,ac^2 + Bc^3) \cdot d^2$$
   to show that $c^3 = d^2$. Hint: d^2 divides the left hand side and c^3 divides the right hand side.

   (b) Then deduce that there is an integer $e > 0$ such that $c = e^2$ and $d = e^3$.

   (c) Show that $P = (ae : b : e^3)$ is a normalised representation of P.

   (d) Prove that x_P and y_P are both integers (we say P is an integral point) if and only if, for all primes p, the reduction $\tilde{P}$ modulo p is different from $(0 : 1 : 0)$.