Elliptic curves: exercise sheet 2

Due: 24th September 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 11.

(a) Show that the ideal $I \subset \mathbf{R}[X,Y]$ generated by $X(X^2+Y^2-1)$ and $Y(X^2+Y^2-1)$ is not prime.

(b) Make a picture of $V(I) \subset \mathbf{R}^2$.

(c) Show that the ideal $J \subset \mathbf{R}[X,Y]$ generated by $Y^2 + X^2 - X^3$ is prime and make a picture of $V(J)$.

Exercise 12. Let k be a field and let I be the homogenous ideal $(Y^2 - ZW, ZX - W^2)$ of the ring $k[X,Y,Z,W]$.

(a) Show that $V(I) \subset \mathbf{P}^3$ is a variety and compute its dimension.

(b) Show that $V(I)$ is not smooth and compute the tangent space in the point $(0:0:1:0)$.

Exercise 13. Let k be a field. A *line* in $\mathbf{P}^2$ is the set of zeroes of a homogenous polynomial in $k[X,Y,Z]$ of degree 1.

(a) Show that a line is a 1-dimensional variety.

(b) Compute the coordinates of the point of intersection of the lines $V(X - Y + Z)$ and $V(2X - Z)$.

(c) Show that any two lines in $\mathbf{P}^2$ have non-empty intersection.

(d) Suppose that k is a finite field of q elements. Determine the number of k-rational points on a line.

Exercise 14. Let $V \subset \mathbf{P}^3$ be the variety of exercise 12. Consider the rational map

$$\phi : V \longrightarrow \mathbf{P}^1$$

given by $\phi(x:y:z:w) = (z:w)$.

(a) Show that there is a unique point Q on V for which $w = z = 0$ and $(z:w)$ does not correspond to a point of $\mathbf{P}^1$.

(b) Show that ϕ is a morphism $V \longrightarrow \mathbf{P}^1$. In other words, there exists g in the function field of V for which either wg or zg does not vanish in Q.

Exercise 15. Let k be a field and let V and W be varieties over k. A morphism $\phi : V \longrightarrow W$ is called an *isomorphism* if there exists a morphism $\psi : W \longrightarrow V$ for which $\phi\psi = \mathrm{id}_W$ and $\psi\phi = \mathrm{id}_V$. Let C be the conic in $\mathbf{P}^2$ given by the equation $Y^2 - XZ = 0$.

(a) Show that the rational map $\phi : C \longrightarrow \mathbf{P}^1$ given by $\phi(x : y : z) = (z : y)$ is an isomorphism.

(b) Show that $\psi : C \longrightarrow \mathbf{P}^1$ given by $\psi(x : y : z) = (z : x)$ is not.

Exercise 16. Let $\mathbf{F}_q$ be a finite field with q elements and let $\varphi : \mathbf{P}^n \longrightarrow \mathbf{P}^n$ denote the *Frobenius morphism*, given by $\varphi(x_0 : x_1 : \ldots : x_n) = (x_0^q : x_1^q : \ldots : x_n^q)$.

(a) Show that φ is indeed a morphism.

(b) Show that φ is a bijection $\mathbf{P}^n(\overline{\mathbf{F}}_q) \longrightarrow \mathbf{P}^n(\overline{\mathbf{F}}_q)$.

(c) Show that φ is not an isomorphism

Exercise 17. Let k be a field of characteristic 3 and let E be the curve in $\mathbf{P}^2$ given by

$$Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

(a) Show that E is an elliptic curve, i.e. E is smooth, if $a_2 = 0$ and $a_4 \neq 0$.

(b) Show that E is an elliptic curve if and only if $a_4^3 - a_2^2a_4^2 + a_6a_2^3 \neq 0$.

Exercise 18. Let k be a field of characteristic ≥ 5, let $A, B \in k$ with $4A^3 + 27B^2 \neq 0$ and let E be the elliptic curve with affine equation $Y^2 = X^3 + AX + B$.

(a) Let $P = (x, y)$ be a point on E. Show that the slope of the tangent line in P is given by $\lambda = (3x^2 + A)/2y$. In particular, if $y = 0$, the tangent line is the vertical line given by the equation $X = x$.

(b) Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points on E. Show that the slope of the line passing through P and Q is given by $\lambda = (y_2 - y_1)/(x_2 - x_1)$. In particular, if $Q = (x_1, -y_1)$, the line is the vertical line given by the equation $X = x_1$.

(c) Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = (x_3, y_3)$ be points on E satisfying $P+Q = R$. Show that

$$x_1 + x_2 + x_3 = \lambda^2, \qquad \text{and} \qquad (-y_3 - y_1)/(x_3 - x_1) = \lambda,$$

where λ is the slope of the line in part (a) or (b) depending on whether $P = Q$ or not.

Exercise 19. Let E be the elliptic curve over $\mathbf{Q}$ given by the equation $Y^2 = X^3 + 17$. Use the formulas of the preceding exercise for the following.

(a) Show that $P = (-2, 3)$, $Q = (-1, 4)$ and $R = (2, -5)$ are points on E.

(b) Show that $P + R = (4, 9)$.

(c) Show that $P + P = (8, -23)$.

(d) Let $3P$ denote the point $P + P + P$. Compute $3P + R$.

(e) Compute $Q - R$.

Exercise 20. Let E be the elliptic curve over $\mathbf{F}_7$ given by the affine equation $Y^2 = X^3 + 2$.

(a) Show that E has precisely nine points defined over $\mathbf{F}_7$.

(b) Decide whether or not $E(\mathbf{F}_7)$ is cyclic or not.