HOMEWORK 2

TOPICS IN AG: ELLIPTIC CURVES

(1) Compute the tangents to the hyperbola $X^2 - Y^2 = 1$ and to the parabola $Y = X^2$ (over the real numbers) at their points at infinity. Use the insight gained to give a definition of the concept of an asymptote for algebraic curves defined over arbitrary (e.g. finite) fields.

The hyperbola has two points $[1 : 1 : 0]$ and $[1 : -1 : 0]$ at infinity for any field of characteristic $\neq 2$. The tangents at infinity are $Y - X = 0$ and $Y + X = 0$, which happen to be the asymptotes of the hyperbola over the reals.

The parabola has one point at infinity, namely $[0 : 1 : 0]$. The tangent there is the line at infinity $Z = 0$.

We could define an asymptote as a tangent at infinity that is different from the line at infinity.

(2) Let K be a field of characteristic $\neq 2$, and $f \in K[X]$ a polynomial of degree ≥ 4 without multiple roots. Show that the projective closure of the hyperelliptic curve $y^2 = f(x)$ has exactly one singular point.

Assume that $r = \deg g \geq 3$. Then the projective closure of $\mathcal{C}$ has the eqation $F(X, Y, Z) = Y^2 Z^{r-2} - G(X, Z) = 0$. For determining its points at infinity, put $Z = 0$; then $0 = F(X, Y, 0) = -G(X, 0) = -a_r X^r$, hence $X = 0$. Thus $P = [0 : 1 : 0]$ is the only point at infinity on $\mathcal{C}^{\#}$.

We claim that P is singular if $r \geq 4$. We get

$$F_X(P) = -\frac{dG}{dX}(0, 0) = 0,$$
$$F_Y(P) = 2YZ^{r-2}|_P = 0.$$

Now $F_Z = (r-2)Y^2 Z^{r-3} - \frac{dG}{dZ}(0, 0)$; the last term is 0, hence $F_Z(P) = 0$ if and only if $r > 3$.

It is easily checked that there is no singular point if $r \leq 2$.

(3) Let $f, g, h \in K[x, y]$ be polynomials, and put $f = gh$. Show that any point of intersection of the curves $g(x, y) = 0$ and $h(x, y) = 0$ is a singular point of the curve $f(x, y) = 0$.

Working projectively, we have to show that the partial derivatives of F vanish for points of intersection. But $F_X = G_X H + G H_X$, and plugging in a point $P = [x : y : z]$ satisfying $G(x, y, z) = H(x, y, z) = 0$ we see that $F_X(P) = 0$. The other derivatives also vanish there.

(4) Show that the Klein quartic

$$X^3Y + Y^3Z + Z^3X = 0$$

defined over a field K is smooth if and only if K has characteristic $\neq 7$.

We first compute derivatives:

$$F_X = 3X^2Y + Z^3,$$
$$F_Y = 3Y^2Z + X^3,$$
$$F_Z = 3Z^2X + Y^3.$$

If K has characteristic 7, then $[1 : 2 : 4]$ is easily checked to be a singular point.

Now assume that K has characteristic $\neq 7$; then for points at which all three derivatives vanish we have $XF_X = 3X^3Y + XZ^3 = -9Y^3Z + XZ^3 = 27XZ^3 + XZ^3 = 28Z^3 = 0$, hence for fields of characteristic $\neq 2, 7$ singular points satisfy $Z = 0$. By symmetry, we also must have $X = Y = 0$, hence there is no singular point in these cases.

Assume that K has characteristic 2; from $XF_X = X^3Y + XZ^3 = Y^3Z$ we get $Y = 0$ or $Z = 0$; this immediately leads to $X = Y = Z = 0$, hence the Klein quartic is smooth over fields of characteristic 2.

(5) Determine the number of points at infinity of the projective closure of the unit circle $x^2 + y^2 = 1$ over the finite fields $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_9$.

The points at infinity $[x : y : 0]$ satisfy $x^2 + y^2 = 0$. There is no solution over $\mathbb{F}_3$; over $\mathbb{F}_5$ there are the points $[1 : 2 : 0]$ and $[1 : 3 : 0]$; finally, writing $\mathbb{F}_9 = \mathbb{F}_3(i)$ we find that the points at infinity are $[1 : i : 0]$ and $1 : -i : 0]$.

Observe that points at infinity are on the line at infinity, and lines intersect conics in at most two points.

(6) Consider the parabola $\mathcal{C} : y = x^2$ over some ring R. Show that the geometric group law defined for conics (with neutral element $N = (0, 0)$)specializes to

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \quad \text{for } x_3 = x_1 + x_2.$$

Deduce that $\mathcal{C}(R) \simeq (R, +)$, the additive group of R.

Assume first that $x_1 \neq x_2$. Then the slope of the line through the two points is given by $m = \frac{y_2 - y_1}{x_2 - x_1} = x_2 + x_1$, and the parallel through $N = (0, 0)$ is $y = (x_2 + x_1)x$. Now x_3 is the nonzero root of the quadratic $x^2 = (x_2 + x_1)x$, i.e., $x = x_2 + x_1$. The cases where $x_1 = x_2$ are equally simple.

Checking that $\phi : (x, y) \longmapsto x$ induces an isomorphism $\mathcal{C}(R) \longrightarrow (R, +)$ is trivial.

(7) Consider the hyperbola $\mathcal{C} : xy = 1$ over some ring R. Show that the geometric group law defined for conics (with neutral element $N = (1, 1)$ specializes to

$$(x_1, y_1) + (x_2 b y_2) = (x_3, y_3) \quad \text{for } x_3 = x_1 x_2.$$

Deduce that $\mathcal{C}(R) \simeq R^\times$, the unit group of R.

Again let me assume that $x_1 \neq x_2$; then the slope is $m = \frac{y_2-y_1}{x_2-x_1} = -\frac{1}{x_1x_2} \in R^\times$, the parallel through N is $y = m(x-1)+1$, hence $1 = xy = x[m(x-1)+1]$ or $(x-1)(mx+1) = 0$; the second point of intersection of $x = -\frac{1}{m} = x_1x_2$.

Clearly the map $\mathcal{C}(R) \longrightarrow R^\times : (x,y) \longmapsto x$ is an isomorphism.

Note: Never use the quadratic formula to compute the root of a quadratic equation if you already know one solution!