Plane Algebraic Curves – Problem Set 6

due Tuesday, July 11

(1) Let F be an elliptic curve of the form

$$F = y^2z - x^3 - \lambda xz^2 - \mu z^3$$

for some given $\lambda, \mu \in K$ (it can be shown that every elliptic curve can be brought into this form by a change of coordinates if the characteristic of K is not 2 or 3). Pick the point $P_0 = (0:1:0) \in F$ as the base point for the group structure on $V(F)$.

For given points P and Q on F compute explicitly the coordinates of the sum $P \oplus Q$ and the inverse $\ominus P$ in terms of the coordinates of P and Q.

(2) Let $F = y^2z - x^3 - \lambda xz^2$ be an elliptic curve as in Exercise 1 with $\mu = 0$, defined over a finite field of characteristic p (so that $\mathbb{Z}/p\mathbb{Z}$ is a subfield of K). Show:

(a) If $p = 3 \mod 4$ then $V(F) \cap \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ contains exactly $p+1$ points.

(b) If $p = 1 \mod 4$ then the number of points of $V(F) \cap \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ may also be smaller or bigger than $p+1$, but is always even.

(3) Let Λ be a lattice in $\mathbb{C}$, and let $P \neq Q$ be points in $\mathbb{C}/\Lambda$. Show that there is no meromorphic function on $\mathbb{C}/\Lambda$ with a simple zero at P, a simple pole at Q, and which is holomorphic with non-zero value at all other points.

(Note that we can view this as an analytic analogue of the statement proven in class that two points $P \neq Q$ on a smooth projective curve F are never linearly equivalent, i. e. that there is no rational function φ on F with $\operatorname{div}\varphi = P - Q$.)

(4) Let F be a smooth projective curve of degree d. For a divisor D on F we set

$$L(D) := \{\varphi \in K(F)^* : \operatorname{div}\varphi + D \geq 0\} \cup \{0\} \quad \subset K(F).$$

Moreover, by V_n we denote the vector space of homogeneous polynomials in x, y, z of degree n. For all $n \geq d$, show for the divisor $D := n \operatorname{div} z$:

(a) $L(D)$ is a vector space fitting into an exact sequence

$$0 \longrightarrow V_{n-d} \xrightarrow{\cdot F} V_n \xrightarrow{:z^n} L(D) \longrightarrow 0.$$

(b) $\dim L(D) = \deg D + 1 - \binom{d-1}{2}$.