

ALGEBRAIC CURVES OVER FINITE FIELDS

Homework 2

The second homework assignment consists in **5 problems** of your choice among those ones listed here below (if you hand in more exercises, I will count the 5 with the highest score). It is **due on Wednesday, November 28**.

Note: This homework assignment is in constant evolution... Problems will be added as the semester goes on, but once an exercise is posted, it will not change (up to ordering). Discussion of the homework problems with me, or collaboration (in a reasonable degree) with your classmates, is encouraged, but you have to provide a note on which problems you had assistance.

Ex 1. In $\mathbb{A}^2(\mathbb{R})$, a **conic** \mathcal{C} is an algebraic set of the form $V(f(x, y))$, where $f(x, y) \in \mathbb{R}[x, y]$ is a polynomial of degree two. In other terms one has:

$$\mathcal{C} : Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0,$$

where $A, B, C, D, E, F \in \mathbb{R}$ and A, B, C are not all zero.

- (a) (Bonus) A conic \mathcal{C} is called non-degenerate if \mathcal{C} is absolutely irreducible, i.e. \mathcal{C} is irreducible over \mathbb{C} . Show that \mathcal{C} is non-degenerate if and only if

$$\begin{vmatrix} A & \frac{B}{2} & \frac{D}{2} \\ \frac{B}{2} & C & \frac{E}{2} \\ \frac{D}{2} & \frac{E}{2} & F \end{vmatrix} \neq 0.$$

- (b) If \mathcal{C} is non-degenerate, then \mathcal{C} can be classified as follows:

- \mathcal{C} is an **ellipse** if and only if $B^2 - 4AC < 0$;
- \mathcal{C} is a **parabola** if and only if $B^2 - 4AC = 0$;
- \mathcal{C} is a **hyperbola** if and only if $B^2 - 4AC > 0$.

Let $\overline{\mathcal{C}} \subseteq \mathbb{P}^2(\mathbb{R})$ be the projective closure of \mathcal{C} . Show that the above classification is equivalent to the following one:

- \mathcal{C} is an ellipse if and only if $\overline{\mathcal{C}}$ has no points at infinity;
- \mathcal{C} is a parabola if and only if $\overline{\mathcal{C}}$ has one point at infinity;
- \mathcal{C} is a hyperbola if and only if $\overline{\mathcal{C}}$ has two different points at infinity.

- (c) Consider the family of conics $\{\mathcal{C}_t\}_{t \in \mathbb{R}}$ where

$$\mathcal{C}_t : x^2 - txy - 8ty^2 - x - y = 0.$$

Classify \mathcal{C}_t with respect to the parameter t , and for $t = 4$ find the points at infinity of $\overline{\mathcal{C}}_4$.

Ex 2. (a) Let $K \subseteq L$ be a separable field extension of degree n . For $i = 1, \dots, n$, let $\sigma_i : L \rightarrow \overline{K}$ be a K -embedding of L into \overline{K} . Prove that $\gamma \in L$ is in K if and only if $\sigma_i(\gamma) = \gamma$, for all $i = 1, \dots, n$.

- (b) Let k be a perfect field and $P \in \mathbb{A}^n(\bar{k})$. Prove that $P \in \mathbb{A}^n(k)$ if and only if $P^\sigma = P$ for all $\sigma \in \text{Gal}_k(\bar{k})$.

Ex 3. Prove that the following conditions are equivalent for a field k .

- (a) Every irreducible polynomial in $k[x]$ is separable.
- (b) Every algebraic extension of k is separable.
- (c) Either k has characteristic 0, or, when k has characteristic $p > 0$, every element of k is a p th power, i.e. for all $\alpha \in k$ there exists $\beta \in k$ such that $\beta^p = \alpha$.
- (d) Either k has characteristic 0, or, when k has characteristic $p > 0$, the Frobenius endomorphism $x \rightarrow x^p$ is an automorphism of k .

You may use the fact that $f(x) \in k[x]$ is separable if and only if $\gcd(f(x), f'(x)) = 1$.