# MATH 115: NOTES ON CURVE THEORY 1

MARTIN OLSSON

## 1. Fields

A *field* is a set $k$ together with two operations

$$+ : k \times k \to k, \quad \cdot : k \times k \to k.$$

For $(a, b) \in k \times k$ we usually write $a + b$ (resp. $a \cdot b$ or just $ab$) for the image of the pair $(a, b)$ under the operation $+$ (resp. $\cdot$). These two operations are required to satisfy the following:

(F1) For any $a, b \in k$ we have

$$a + b = b + a, ab = ba.$$

(F2) There exists an element $0 \in k$ (resp. $1 \in k$) such that for any $a \in k$ we have

$$a + 0 = 0 + a = a, \quad 1 \cdot a = a \cdot 1 = a.$$

Note that the elements 0 and 1 are unique.

(F3) For any $a \in k$ there exists a unique element $a' \in k$

$$a + a' = 0.$$

We usually write $-a$ for the element $a'$.

(F4) For any $a \in k$ which is not equal to 0, there exists a unique element $b \in k$ such that

$$ab = 1.$$

We usually write $a^{-1}$ for this element.

(F5) For any $a, b, c \in k$ we have

$$a + (b + c) = (a + b) + c, \quad a(bc) = (ab)c, \quad a(b + c) = ab + ac.$$

**Example 1.1.** Some examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. If $p$ is a prime then the congruence classes modulo $p$ form a field under addition and multiplication of congruence classes. This field is usually denoted $\mathbb{F}_p$ (sometimes also written $\mathbb{Z}/(p)$).

We can talk about polynomials $F$ with coefficients in a field $k$. Such a polynomial (in variables $X_1, \ldots, X_n$ say) is simply a finite sum of monomial terms

$$a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n},$$

with each $i_j \geq 0$.

Given a vector $(s_1, \ldots, s_n) \in k^n$ and a polynomial

$$F = \sum_{\underline{i}} a_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n}$$

we define
$$F(s_1, \ldots, s_n) := \sum_{\underline{i}} a_{\underline{i}} s_1^{i_1} \cdots s_n^{i_n} \in k.$$

A polynomial $F$ in variables $X_1, \ldots, X_n$ is called *homogeneous of degree* $r$ if for each monomial $X_1^{i_1} \cdots X_n^{i_n}$ occurring in $F$ we have
$$i_1 + \cdots + i_n = r.$$

## 2. Projective space

Let $k$ be a field, and let $n \geq 0$ be an integer. Define *$n$-dimensional projective space* $\mathbb{P}^n(k)$ *over* $k$ as follows. The set $\mathbb{P}^n(k)$ is the set of equivalence classes of vectors
$$(a_0, \ldots, a_n)$$
of elements $a_i \in k$, such at least one $a_i$ is nonzero. Two vectors $(a_0, \ldots, a_n)$ and $(a_0', \ldots, a_n')$ are declared equivalent if there exists a nonzero element $\lambda \in k$ such that
$$a_i = \lambda a_i'$$
for all $i$. We usually write
$$[a_0 : \cdots : a_n]$$
for the equivalence class of the vector $(a_0, \ldots, a_n)$.

We write $\mathbb{A}^n(k) \subset \mathbb{P}^n(k)$ for the subset of points $[a_0 : \cdots : a_n]$ with $a_n \neq 0$. Note that we have a bijection
$$k^n \rightarrow \mathbb{A}^n(k), \quad (b_0, \ldots, b_{n-1}) \mapsto [b_0 : \cdots b_{n-1} : 1].$$

If $F$ is a homogeneous polynomial of degree $r$ in variables $X_0, \ldots, X_n$ then for any $\lambda \in k$ and vector $(a_0, \ldots, a_n)$ we have
$$F(\lambda a_0, \ldots \lambda a_n) = \lambda^n F(a_0, \ldots, a_n).$$
It therefore makes sense to say that $F$ vanishes on a point $[a_0 : \cdots : a_n]$ of $\mathbb{P}^n(k)$. If $F_1, \ldots, F_t$ are homogeneous polynomials we define
$$V(F_1, \ldots, F_t) \subset \mathbb{P}^n(k)$$
to be the set
$$V(F_1, \ldots, F_t) = \{[a_0 : \cdots : a_n] | F_j([a_0 : \cdots : a_n]) = 0 \ \text{ for all } j\}.$$

**Example 2.1.** Consider the subset
$$V(X^2 + Y^2 - Z^2) \subset \mathbb{P}^n(k).$$
The intersection of $V(X^2 + Y^2 - Z^2) \cap \mathbb{A}^2(k) = k^2$ is the set of solutions to the equation
$$X^2 + Y^2 = 1.$$
The points in $\mathbb{P}^2(k) - \mathbb{A}^2(k)$ is the set
$$V(X^2 + Y^2) \subset \mathbb{P}^1(k),$$
where $\mathbb{P}^1(k)$ is embedded in $\mathbb{P}^2(k)$ via the map
$$\mathbb{P}^1(k) \rightarrow \mathbb{P}^2(k), \quad [a : b] \mapsto [a : b : 0].$$

## 3. Homogenizing equations

We will often consider the following situation. Let

$$f = \sum_{i,j} a_{i,j} X^i Y^j$$

be a polynomial in two variables defining a subset

$$\{(a,b) \in k^2 | f(a,b) = 0\} \subset k^2.$$

We can extend this zero set to all of $\mathbb{P}^2(k)$ as follows. Let $r$ be the maximum of the integers $i+j$ for $X^iY^j$ a nonzero monomial occurring in $f$. Then define

$$F := \sum_{i,j} a_{i,j} X^i Y^j Z^{r-i-j},$$

a homogeneous polynomial in three variables. The resulting zero set

$$V(F) \subset \mathbb{P}^2(k)$$

then has the property that $V(F) \cap \mathbb{A}^2(k)$ is the original set of zeros of $f$. The polynomial $F$ is called the homogenization of $f$.

More generally one can consider polynomials in more variables and zero sets of several polynomials at a time.

**Example 3.1.** If

$$f = Y^2 - X^3 - aX - b$$

for some constants $a, b \in k$ then the homogenization of $f$ is the polynomial

$$F = Y^2Z - X^3 - aXZ^2 - bZ^3.$$

Note that the points at infinity of $V(F)$ consist of triples $[\alpha : \beta : 0]$ for which

$$-\alpha^3 = 0.$$

This implies that $\alpha = 0$ so the only point at infinite is $[0 : 1 : 0]$. This is an important example, and is an example of an elliptic curve.

## 4. Exercises

**Exercise 1.** For which integers $m$ is the set of congruence classes modulo $m$ a field (under addition and scalar multiplication of congruence classes)?

**Exercise 2.** Let $k$ be a field. Show that there is a natural decomposition

$$\mathbb{P}^n(k) = k^n \cup k^{n-1} \cup \cdots \cup k \cup \{*\}.$$

In particular, show that

$$\mathbb{P}^n(\mathbb{F}_p)$$

consists of

$$p^n + p^{n-1} + \cdots + p + 1 = (p^{n+1} - 1)/(p-1)$$

elements.

**Exercise 3.** Exhibit a natural bijection between $\mathbb{P}^n(\mathbb{R})$ and the set of lines in $\mathbb{R}^{n+1}$ which pass through $(0, \ldots, 0) \in \mathbb{R}^{n+1}$.