Chapter 3

Projective Spaces

3.1 The Projective Line

Suppose you want to describe the lines through the origin $O = (0,0)$ in the Euclidean plane $\mathbb{R}^2$. The first thing you might think of is to write down the equation $y = mx$, but then you are told that this does not cover the line $x = 0$. The second idea is to consider all the equations $ax + by = 0$ with $(a,b) \neq (0,0)$, and these do indeed describe all lines through O; on the other hand, one and the same line like $y = x$ is described by infinitely many different equations, namely $ax - ay = 0$ for any $a \neq 0$. More generally, two lines $ax + by = 0$ and $a'x + b'y = 0$ will represent the same lines if $(a', b') = (\lambda a, \lambda b)$ for some nonzero λ.

In order to get the best of both worlds, we define an equivalence relation on the set of all points $(a,b) \neq (0,0)$ by saying that $(a,b) \sim (a',b')$ if $(a',b') = (\lambda a, \lambda b)$ for some nonzero λ. The equivalence class of (a,b) is denoted by $[a:b]$, and the set of all equivalence classes is called the real projective line $\mathbb{P}^1\mathbb{R}$.

The same construction works for general fields: we put $\mathbb{P}^1 K = (K \times K \setminus \{(0,0)\})/\sim$, where the equivalence relation $\sim$ is defined exactly as above. The space $\mathbb{P}^1 K$ (occasionally also denoted by $K\mathbb{P}^1$) is called the projective line over K.

Note that $\mathbb{P}^1 K$ is called the projective *line* even though each point is represented by two coordinates: this is because the projective line is, up to some mysterious "point at infinity", the same as the affine line $\mathbb{A}^1 K = K$. In fact, $a \longmapsto [a : 1]$ defines a map $\iota : \mathbb{A}^1 K \longrightarrow \mathbb{P}^1 K$ which is clearly injective: $\iota(a) = \iota(b)$ means that $[a : 1] = [b : 1]$, hence there exists a nonzero $\lambda \in K$ with $a' = \lambda a$, $1 = \lambda 1$, which implies $\lambda = 1$ and then $a = a'$, $b = b'$. Moreover, ι is almost surjective: the only points on the projective line not in the image are those of the form $[a : 0]$ with $a \neq 0$ (recall that there is no such thing as $[0 : 0]$). But if $a \neq 0$, then $[a : 0] = [1 : 0]$, which means $\mathbb{P}^1 K = \mathbb{A}^1 K \cup \{[1 : 0]\}$. Thus we can identify the points $\neq [1 : 0]$ on the projective line with the usual affine points, and we call the additional point $[1 : 0]$ the point at infinity on $\mathbb{P}^1 K$.

In our example with lines through the origin, we now can identify the line $ax + by = 0$ with the point $[a : b]$, since this is a bijection: equations describing the same line correspond to the same point on the projective line. The line $ax + by = 0$ has slope $m = -a/b$ if $b \neq 0$; if you let $b \longrightarrow 0$, the slope will tend to infinity, and in the limit you get the line $x = 0$ and the point $[1 : 0] \in \mathbb{P}^1 K$.

3.2 Lifting Maps from the Affine to the Projective Line

In calculus you studied real-valued functions on the real line $\mathbb{R} = \mathbb{A}^1 R$. Now we can study rational functions $\mathbb{P}^1 K \longrightarrow \mathbb{P}^1 K$. In fact, consider the rational function $f(x) = \frac{2x-1}{x-2}$. Clearly $f(3) = 5$; since f has a pole at $x = 2$, we are tempted to put $f(2) = \infty$. Can we make this precise?

Yes we can. The function $f : x \longmapsto \frac{2x-1}{x-2}$ is defined on the real line except for $x = 2$; we can map $f(x)$ to the projective line with ι and then get $\iota(f(x)) = [\frac{2x-1}{x-2} : 1]$. For $x \neq 2$, however, we have $[\frac{2x-1}{x-2} : 1] = [2x-1 : x-2]$, so we might just as well put $\iota(f(x)) = [2x - 1 : x - 2]$. But this does even make sense for $x = 2$, so $f(2)$ gets mapped to $[3 : 0] = [1 : 0] \in \mathbb{P}^1 K$, that is, to the point at infinity.

This makes f into a map $\mathbb{A}^1 K \longrightarrow \mathbb{P}^1 K$. Can we also extend the domain of f to the projective line? In other words, can we make some sense of $f(\infty)$? If you remember your calculus, you probably will guess that we should have $f(\infty) = \lim_{x\to\infty} f(x) = 2$. The only problem is that, in fields $K \neq \mathbb{R}$, we don't have the notion of a limit. What we can do is the following: first observe that we can identify x with $[x : 1]$, hence we can put $f([x : 1]) = f(x)$. In order to get a good definition for $f([x : 0])$ we substitute $x = \frac{s}{t}$ and observe $[x : 1] = [\frac{s}{t} : 1] = [s : t]$; this gets mapped to $[2x-1 : x-2] = [2\frac{s}{t}-1 : \frac{s}{t}-2] = [2s-t : s-2t]$. Thus we finally arrive at the map

$$\mathbb{P}^1 K \longrightarrow \mathbb{P}^1 K : [s : t] \longmapsto [2s - t : s - 2t].$$

In fact we have $f([1 : 0]) = [2 : 1]$, that is, $f(\infty) = 2$.

Is it possible to "extend" the domain and codomain of functions in general? The answer is yes for rational functions. In order to be able to state this concisely, let us introduce the homogenization of a polynomial $f \in K[x]$: if

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

and $a_n \neq 0$, then the polynomial

$$F(X, Y) = a_n X^n + a_{n-1}X^{n-1}Y \ldots + a_1 XY^{n-1} + a_0 Y^n$$

is called the homogenization of f. In other words: we put

$$F(X, Y) = Y^{\deg f} f\big(XY^{-1}\big).$$

Lemma 3.2.1. *If G is the homogenization of g, then*

- $G(\lambda X, \lambda Y) = \lambda^{\deg g} G(X, Y)$;
- $G(x, 1) = g(x)$.

In our example above, the extension of the rational map $f = \frac{g}{h}$ to the projective line was given by $F[s : t] = [G(s,t) : H(s,t)]$, where $G(X,Y) = 2X - Y$ and $H(X,Y) = X - 2Y$ were the homogenizations of g and h. In general, however, we cannot simply define F like this, as the example $f(x) = \frac{x-1}{x^2}$ shows: the map $[s : t] \longmapsto [s - t : t^2]$ is not well defined! The solution is to define the projective extension here as $[s : t] \longmapsto [st - t^2 : t^2]$.

Proposition 3.2.2. *Assume that $f : \mathbb{A}^1 K \longrightarrow \mathbb{A}^1 K$ is a rational map (possibly undefined at finitely many points), that is, $f(x) = \frac{g(x)}{h(x)}$ for coprime polynomials $g, h \in K[t]$. Then there is a polynomial map $F : \mathbb{P}^1 K \longrightarrow \mathbb{P}^1 K$ that extends f in the sense that $f(x) \in K$ can be identified with $F([x : 1]) \in \mathbb{P}^1 K$; in fact, we put $a = \deg g - \deg h$ and have*

$$F[s : t] = \begin{cases} [G(s,t) : t^a H(s,t)] & \text{if } a \geq 0, \\ [t^{-a} G(s,t) : H(s,t)] & \text{if } a < 0, \end{cases}$$

where G and H are the homogenizations of G and H.

Proof. The first thing that we should check is whether the map is well defined. What happens if we replace (s,t) by $(\lambda s, \lambda t)$? The left hand side of course does not change, but on the right hand side we get, in the case $a = \deg g - \deg h \geq 0$,

$$\begin{aligned} [G(\lambda s, \lambda t) : \lambda^a t^a H(\lambda s, \lambda t)] &= [\lambda^{\deg g} G(s,t) : \lambda^{a + \deg h} t^a H(s,t)] \\ &= [G(s,t) : t^a H(s,t)] \end{aligned}$$

as desired. The case $a < 0$ is handled similarly.

We also have to check that $F([s : t]) \in \mathbb{P}^1 K$, i.e., that (in the case $a \geq 0$) $G(s,t)$ and $t^a H(s,t)$ cannot simultaneously vanish. To this end, assume that there is a point $[s : t] \in \mathbb{P}^1 K$ with $G(s,t) = t^a H(s,t) = 0$. If $t \neq 0$, then we may assume that $t = 1$, and we find $G(s,1) = g(s)$ and $H(s,1) = h(s)$. If these values are both 0, then $f - \frac{g}{h}$ was not in lowest terms since $g(x)$ and $h(x)$ share the common factor $x - s$. If $t = 0$, then $G(s,0) = 0$, which implies that $s = 0$, and this is a contradiction since $[0 : 0] \notin \mathbb{P}^1 K$.

Next we have to check that $F([x : 1]) = [f(x) : 1]$ for all $x \in K$ at which f is defined. In fact, we get (again in the case $a \geq 0$)

$$F([x : 1]) = [G(x,1) : H(x,1)] = [g(x) : h(x)] = [f(x) : 1].$$

Thus F coincides with f on the affine part of the projective line. □

3.3 Projective Planes

We now can define the projective plane in a similar way: on the set $K^3 \setminus \{(0,0,0)\}$ of all nonzero 3-tuples with entries from K introduce an equivalence relation via $(a,b,c) \sim (a',b',c')$ if there is a $\lambda \in K^\times$ such that $a' = \lambda a$, $b' = \lambda b$, $c' = \lambda c$. The equivalence class of (x,y,z) is denoted by $[x:y:z]$, and the set of all equivalence classes is called the projective plane $\mathbb{P}^2K$.

Just as the affine line can be embedded in to the projective line, the affine plane $\mathbb{A}^2K = K \times K$ can be viewed as being a part of the projective plane: the map

$$\iota : \mathbb{A}^2K \longrightarrow \mathbb{P}^2K; (a,b) \longmapsto [a:b:1]$$

is injective. In fact, if $[a:b:1] = [a':b':1]$, then by definition of equality in $\mathbb{P}^2K$ there is a $\lambda \in K^\times$ such that $a' = \lambda a$, $b' = \lambda b$, and $1 = \lambda \cdot 1$. The last equation gives $\lambda = 1$, hence $(a,b) = (a',b')$.

As for the line, the map ι is not surjective: there are points in the projective plane that cannot be seen in the affine picture. These 'points at infinity' are the points $[a:b:0]$ for $a,b \in K$ not both 0. These consist of the set $\{[a:1:0]; a \in K\}$ and the point $[1:0:0]$, hence we can write

$$\mathbb{P}^2K = \iota(\mathbb{A}^2K) \cup \{[a:1:0]; a \in K\} \cup \{[1:0:0]\}.$$

3.4 Projective Closure of Lines

Using the embedding $\mathbb{A}^2K \longrightarrow \mathbb{P}^2K$ we can, of course, also embed algebraic curves. Consider the simplest example, that of a line $L : ax + by + c = 0$. Any point $P = (x,y)$ on L will get mapped to $\iota(P) = [x:y:1] \in \mathbb{P}^1K$. This point has different presentations; we can write it as $\iota(P) = [\lambda x : \lambda y : \lambda]$ for any $\lambda \in K^\times$. These coordinates all satisfy the equation $aX + bY + cZ = 0$: in fact,

$$a(\lambda x) + b(\lambda y) + c(\lambda) = \lambda(ax + by + c) = 0.$$

We call the set of all points $[X:Y:Z]$ in the projective plane satisfying $aX + bY + cZ = 0$ the projective closure of the line L and denote it by $L^\#$. The zero set of any equation $aX + bY + cZ = 0$ with $(a,b,c) \neq (0,0,0)$ is called a projective line.

Let us now investigate what the points at infinity on this line $L^\#$ are; all we have to do is put $Z = 0$ in the equation of the projective line: we get $ax + by = 0$. We cannot have $a = b = 0$, since $ax + by + c = 0$ was supposed to be a line. Now $ax + by = 0$ has the general solution $(x,y) = (\lambda b, -\lambda a)$ for $\lambda \in K$. Thus the only point at infinity on $L^\#$ is the point $[b : -a : 0]$.

Proposition 3.4.1. *The projective closure of an affine line has exactly one point at infinity.*

The "line" $\{[x:1:0]; x \in K\}$ that we were talking about before is a projective line: it is described as the set of projective solutions of $z = 0$ and is called the line at infinity. We have just seen that every affine line $L : ax+by+c = 0$ intersects the line at infinity in exactly one point $[b : -a : 0]$. Note that, if $b \neq 0$, then $m = -a/b$ is the slope of the line L, and $[1 : m : 0]$ is its point at infinity. Thus every affine line with slope m intersects the line at infinity at

$[1 : m : 0]$. In particular, every pair of parallel lines has a point of intersection at infinity, and we have

Proposition 3.4.2. *Two distinct projective lines have exactly one point of intersection.*

This is of course the most special case of Bezout's theorem that you can imagine (Bezout's theorem states that two curves of degree m and n without common components intersect in exactly mn points, counting multiplicity).

The notion of projective closure makes sense for arbitrary affine curves $\mathcal{C}$ given by $f(x, y) = 0$ for some $f \in K[x, y]$; the image of a point $P = (x, y) \in \mathcal{C}(K)$ in the projective plane, namely $\iota(P) = [x : y : 1]$, satisfies the equation $F(X, Y, Z) = 0$, where F is the homogenization of f defined by $F(X, Y, Z) = Z^{\deg f} f(\frac{X}{Z}, \frac{Y}{Z})$. Note that the degree of $x^a y^b$ is $a + b$.

3.5 Parametrization of the Unit Circle

Now let us have a second look at the parametrization of the unit circle $\mathcal{C} : x^2 + y^2 = 1$. We found that the map

$$\phi : \mathbb{A}^1\mathbb{Q} \longrightarrow \mathcal{C} \subseteq \mathbb{A}^2\mathbb{Q} : t \longmapsto \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)$$

gave us all rational points on the unit circle except $P = (-1, 0)$, which – intuitively – would correspond to the value $t = \infty$: but ∞ is not an element of $\mathbb{A}^1\mathbb{Q}$

On the other hand, in $\mathbb{P}^1\mathbb{Q}$ we have a point at infinity. Let us now see whether we can extend the map ϕ to a map between the projective line and the (projective) unit circle. First we clear denominators and set

$$t \longmapsto (1 - t^2 : 2t : 1 + t^2).$$

Next we write $t = \frac{m}{n}$ as a fraction and send t to $[n^2 - m^2, 2mn, n^2 + m^2]$; thus we are led to define the map

$$\phi^{\#} : \mathbb{P}^1\mathbb{Q} \longrightarrow \mathcal{C} \subseteq \mathbb{P}^2\mathbb{Q} : [m : n] \longmapsto [n^2 - m^2, 2mn, n^2 + m^2].$$

This is actually a bijection between the projective line over $\mathbb{Q}$ and the rational points on the unit circle! In fact, $P = (-1, 0)$ is, in its projective incarnation $[-1 : 0 : 1]$, the image of $[m : n] = [-1, 0]$, the point at infinity.

What you can see in this simple example is happening all over the place: results of affine geometry become much simpler if they are stated (and proved) in projective spaces.

3.6 Projective Closure of Conics and Cubics

Consider a curve $\mathcal{C}$ defined by the equation $f(x, y) = 0$. After embedding it via $(x, y) \longmapsto [x : y : 1]$ into the projective plane, the points $[x : y : 1]$ on $\mathcal{C}$

still satisfy the equation $f(x, y) = 0$, but this equation does not behave well with respect to rescaling: we have $[x : y : 1] = [\lambda x : \lambda y : \lambda]$ for nonzero λ, but $f(\lambda x, \lambda y) \neq 0$ in general. The solution is to homogenize f by multiplying each term in f by the power of Z that gives each term the same degree: if $f(x, y) = \sum a_{ij} x^i y^j$, put $F(X, Y, Z) = \sum a_{ij} X^i Y^j Z^k$, where $k = \deg f - i - j$. Then each term of F has degree $\deg f$, and F has the property $F(\lambda X, \lambda Y, \lambda Z) = \lambda^{\deg F} F(X, Y, Z)$. We say that

$$F(X, Y, Z) = Z^{\deg f} f\Big(\frac{X}{Z}, \frac{Y}{Z}\Big)$$

is the homogenization of f. The points $[x : y : 1]$ with $F(x, y, 1) = 0$ are exactly those satisfying $f(x, y) = 0$. The projective curve $\mathcal{C}^\# : F(X, Y, Z) = 0$ is called the projective closure of $\mathcal{C}$, and consists of the affine part $\mathcal{C}$ as well as some (possibly none) points at infinity.

Now consider the three types of conics over $K = \mathbb{R}$:

1. the ellipse $x^2 + y^2 = 1$;
2. the parabola $y^2 = x$;
3. the hyperbola $x^2 - y^2 = 1$.

The projective closure of the circle is the zero set of $X^2 + Y^2 - Z^2 = 0$, its points at infinity satisfy $Z = 0$ and $X^2 + Y^2 = 0$; since $[0 : 0 : 0]$ is not part of $\mathbb{P}^2 K$, the real circle does not have any points at infinity.

The points at infinity of the projective closure $\mathcal{C}^\# : YZ - X^2 = 0$ of the parabola satisfy $Z = 0$ and $X = 0$; there is only one such point, namely $[0 : 1 : 0]$, and this point is indeed a point at infinity on $\mathcal{C}^\#$.

Finally, the hyperbola has two points at infinity, namely $[1 : 1 : 0]$ and $[1 : -1 : 0]$. Note that these points coincide with the points at infinity of the lines $y = x$ and $y = -x$: these are exactly the asymptotes of the hyperbolas, and the asymptotes intersect the hyperbola at infinity.

We can use these facts to *define* that an affine conic defined over a finite field is an ellipse, a parabola or a hyperbola according as it has no, one, or two points at infinity.

For example, if $[x : y : 0]$ is a point at infinity on $\mathcal{C} : x^2 + y^2 = 1$, then $x^2 + y^2 = 0$; thus $\mathcal{C}$ does not have a point at infinity over $\mathbb{F}_3$ (hence is an ellipse over $\mathbb{F}_3$), but has two points at infinity over $\mathbb{F}_5$, namely $[1 : 2 : 0]$ and $[1 : -2 : 0]$, and therefore $\mathcal{C}$ is a hyperbola over $\mathbb{F}_5$. Question: isn't $[2 : 1 : 0]$ a third point at infinity on $\mathcal{C}$?

3.7 Projective Closure of Weierstrass Cubics

Now consider a Weierstrass cubic

$$E : y^2 + a_1 y + a_3 xy = x^3 + a_2 x^2 + a_4 x + a_6.$$

The homogenization of the defining equation is

$$E^{\#} : Y^2Z + a_1YZ^2 + a_3XYZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Putting $Z = 0$ gives $X^3 = 0$, hence the only point at infinity on $E^{\#}$ is $[0 : 1 : 0]$. Thus every Weierstrass curve has a single point at infinity, and this point is K-rational (has coordinates in K) for any field K.