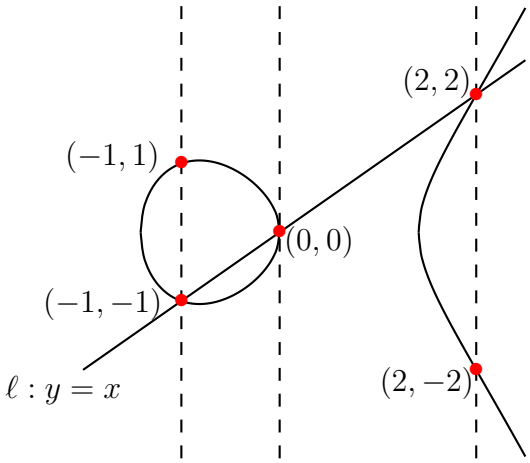


Figure 2.7: Addition in $\mathbb{R}$.

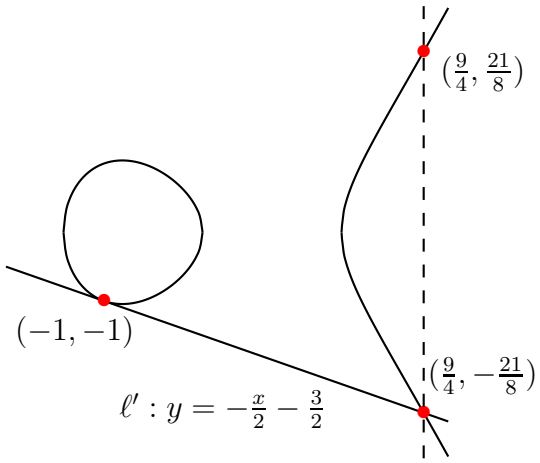


Figure 2.8: Doubling in $\mathbb{R}$.

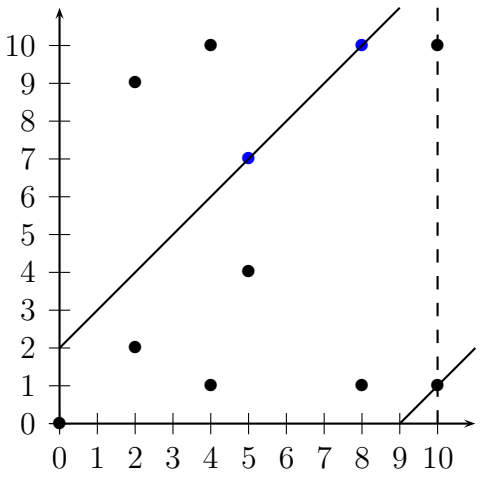
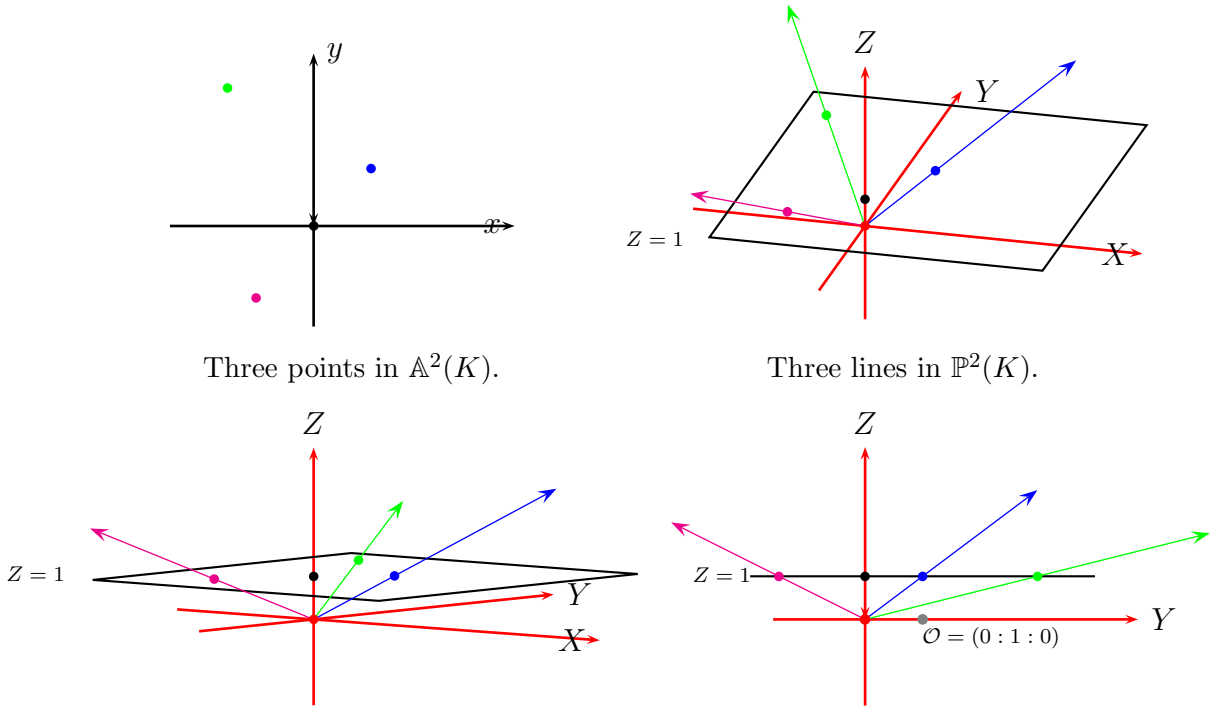


Figure 2.9: The points (excluding $\mathcal{O}$) on $E(\mathbb{F}_{11})$.

2.1.1 The point at infinity in projective space

We now focus our attention on giving a more formal definition for the point at infinity. So far we have been describing elliptic curves in *affine space* as a set of affine points together with the point at infinity: $E = \{(x, y) \in \mathbb{A}^2(\overline{K}) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$. In general, a more precise way to unify (or include) points at infinity with the affine points is to work in *projective space*: essentially, instead of working with points in n-space, we work with lines that pass through the origin in $(n+1)$-space. For our purposes, this means our affine points in 2-space become lines in 3-space, namely that $(x, y) \in \mathbb{A}^2(\overline{K})$ corresponds to the line defined by all points of the form $(\lambda x, \lambda y, \lambda) \in \mathbb{P}^2(\overline{K})$, where $\lambda \in \overline{K}^*$. That is, $\mathbb{P}^2$ is $\mathbb{A}^3 \setminus$

$\{(0,0,0)\}$ modulo the following congruence condition: $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if there exists $\lambda \in \overline{K}^*$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. Figure 2.10 illustrates the relationship between points in $\mathbb{A}^2$ with their congruence classes (lines) in $\mathbb{P}^2$; the lines in 3-space should also extend "downwards" into the region where $Z < 0$ but we omitted this to give more simple pictures. We reiterate that these lines do not include the point $(0, 0, 0)$.



Three points in $\mathbb{A}^2(K)$. Three lines in $\mathbb{P}^2(K)$.

Three lines in $\mathbb{P}^2(K)$. Three lines in $\mathbb{P}^2(K)$.

Figure 2.10: Identifying points in $\mathbb{A}^2$ with lines in $\mathbb{P}^2$

We usually use capital letters and colons to denote a (representative of a) congruence class in projective coordinates, so that in general $(X : Y : Z)$ represents the set of all points on the "line" in $\mathbb{P}^2$ that correspond to $(x, y) \in \mathbb{A}^2$. There are many copies of $\mathbb{A}^2$ in $\mathbb{P}^2$, but we traditionally map the affine point $(x, y) \in \mathbb{A}^2$ to projective space via the trivial inclusion $(x, y) \mapsto (x : y : 1)$, and for any $(X : Y : Z) \neq \mathcal{O} \in \mathbb{P}^2$, we map back to $\mathbb{A}^2$ via $(X : Y : Z) \mapsto (X/Z, Y/Z)$. The point at infinity $\mathcal{O}$ is represented by $(0 : 1 : 0)$ in projective space (see the last diagram in Figure 2.10), for which we immediately note that the map back to $\mathbb{A}^2$ is ill-defined.

Example 2.1.3 (Magma script). $E/\mathbb{R} : y^2 = x^3 + 3x$ is an elliptic curve. $P =$

$(3,6) \in \mathbb{A}^2(\overline{\mathbb{R}})$ is a point on E. In projective space, P becomes $P = (3 : 6 : 1) \in \mathbb{P}^2(\overline{\mathbb{R}})$, which represents all points in $(3\lambda, 6\lambda, \lambda)$ for $\lambda \in \overline{\mathbb{R}} \setminus \{0\}$. For example, the points $(12, 24, 4)$, $(-3\sqrt{-1}, -6\sqrt{-1}, -1\sqrt{-1})$, $(3\sqrt{2}, 6\sqrt{2}, \sqrt{2})$ in $\mathbb{A}^3(\overline{\mathbb{R}})$ are all equivalent (modulo the congruence condition) in $\mathbb{P}^2(\overline{\mathbb{R}})$, where they are represented by P. As usual, the point at infinity on E is $\mathcal{O} = (0 : 1 : 0)$.

The way we define the collection of points in projective space is to *homogenise* $E : y^2 = x^3 + ax + b$ by making the substitution $x = X/Z$ and $y = Y/Z$, and multiplying by Z^3 to clear the denominators, which gives

$$E_{\mathbb{P}} : Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{2.3}$$

The set of points (X, Y, Z) with coordinates in $\overline{K}$ that satisfies (2.3) is called the *projective closure* of E. Notice that $(0, \lambda, 0)$ is in the projective closure for all $\lambda \in \overline{K}^*$, and that all such points cannot be mapped into $\mathbb{A}^2$, justifying the representative of point at infinity being $\mathcal{O} = (0 : 1 : 0)$.

Example 2.1.4 (Magma script). Consider $E/\mathbb{F}_{13} : y^2 = x^3 + 5$. There are 15 affine points $(x, y) \in \mathbb{A}^2(\mathbb{F}_{13})$ on E, which (with the point at infinity $\mathcal{O}$) gives $\#E(\mathbb{F}_{13}) = 16$. On the other hand, if we homogenise (or projectify) E to give $E_{\mathbb{P}}/\mathbb{F}_{13} : Y^2Z = X^3 + 5Z^3$, then there are 16 classes $(X : Y : Z) \in \mathbb{P}^2(\mathbb{F}_{13})$: $(0 : 1 : 0)$, $(2 : 0 : 1)$, $(4 : 2 : 1)$, $(4 : 11 : 1)$, $(5 : 0 : 1)$, $(6 : 0 : 1)$, $(7 : 6 : 1)$, $(7 : 7 : 1)$, $(8 : 6 : 1)$, $(8 : 7 : 1)$, $(10 : 2 : 1)$, $(10 : 11 : 1)$, $(11 : 6 : 1)$, $(11 : 7 : 1)$, $(12 : 2 : 1)$, $(12 : 11 : 1)$. Each of these classes represents several points $(X, Y, Z) \in \mathbb{A}^3(\mathbb{F}_{13})$ whose coordinates satisfy $Y^2Z = X^3 + 5Z^3$ (there are actually 195 such points, but this is not important). In fact, each class represents infinitely many points on $E_{\mathbb{P}}(\overline{\mathbb{F}}_{13})$. Any reader that is familiar with Magma, or has been working through our examples with the accompanying Magma scripts, will recognise the representation of points as representatives in $\mathbb{P}^2$.

The projective coordinates (X, Y, Z) used to replace the affine coordinates (x, y) above are called *homogenous projective coordinates*, because the projective version of the curve equation in (2.3) is homogeneous. These substitutions ($x = X/Z$, $y = Y/Z$) are the most simple (and standard) way to obtain projective coordinates, but we are not restricted to this choice of substitution. For example, many papers in ECC have explored more general substitutions of the form $x = X/Z^i$ and $y = Y/Z^j$ on various elliptic curves [BL07a].

Example 2.1.5 (Magma script). Consider $E/\mathbb{F}_{41} : y^2 = x^3 + 4x - 1$. Using