2. Examples of Conics

Our primary objects of study in this book are conics. As we will see, the set of rational points on conics with at least one such rational point carries a group structure. The two simplest examples are the parabola and the hyperbola, where the group structure turns out to be the additive group and the unit group of the underlying ring. The unit circle, perhaps the simplest conic from a geometric point of view, has a more interesting group structure.

Before we come to the geometric interpretations of the group laws we will be studying, let us briefly review the necessary abstract nonsense: the most basic notions of group theory.

2.1. Groups

Where we go abstract.

The readers already familiar with the notions of groups and homomorphisms may skip this section; the others are invited to do the same and come back here as soon as they stumble across something they do not know.

Recall that a **group** is a set G endowed with a composition $G \times G \longrightarrow G$ sending $a, b \in G$ to $a \circ b \in G$, such that the following properties are verified:

1. Existence of a unit: there is an element $e \in G$ such that $e \circ a = a \circ e = a$ for all $a \in G$.
2. Existence of an inverse: for every $a \in G$ there is a $b \in G$ such that $a \circ b = 1$.
3. Associativity: we have $a(bc) = (ab)c$ for all $a, b, c \in G$.

The most basic mathematical objects in everday life are the natural numbers 1, 2, 3, ... used for counting. The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of natural numbers has a composition called addition, but it does not form a group with respect to addition even if we include 0 (which mathematicians tend to do although historically the invention of 0 came long after the concept of numbers had been discovered). The problem is that the numbers 1, 2, 3, ... do not have additive inverses: there are no natural numbers x such that $x + 1 = 0$. The fact that such inverses are useful in everday life for describing objects that you do not possess (debts etc.) made Indian mathematician invent negative numbers. In mathematical terms, they have completed the semigroup $\mathbb{N}$ to the group $\mathbb{Z}$ of integers.

Most groups we shall deal with will be **commutative**: these are groups satisfying $a \circ b = b \circ a$ for all $a, b \in G$. Commutative groups are usually called **abelian**.

In many cases, the composition is either some form of addition or multiplication. If we write G additively ($a \circ b = a + b$), then we denote the neutral element e by 0, and the inverse of a by $-a$. If we write G multiplicatively, then the neutral element is denoted by 1 and the inverse of a by a^{-1}.

The number of elements of G is denoted by $|G|$ or $\#G$; groups with finitely many elements are called **finite groups**. The most important example of an infinite group is