VI
Elliptic Curves

In recent years a topic in number theory and algebraic geometry — elliptic curves (more precisely, the theory of elliptic curves defined over finite fields) — has found application in cryptography. The basic reason for this is that elliptic curves over finite fields provide an inexhaustible supply of finite abelian groups which, even when large, are amenable to computation because of their rich structure. Before (§ IV.3) we worked with the multiplicative groups of fields. In many ways elliptic curves are natural analogs of these groups; but they have the advantage that one has more flexibility in choosing an elliptic curve than in choosing a finite field.

We shall start by presenting the basic definitions and facts about elliptic curves. We shall include only the minimal amount of background necessary to understand the applications to cryptography in §§2–4, emphasizing examples and concrete descriptions at the expense of proofs and generality. For systematic treatments of the subject, see the references at the end of §1.

1 Basic facts

In this section let K be a field. For us, K will be either the field $\mathbf{R}$ of real numbers, the field $\mathbf{Q}$ of rational numbers, the field $\mathbf{C}$ of complex numbers, or the finite field $\mathbf{F}_q$ of $q = p^r$ elements.

Definition. Let K be a field of characteristic $\neq 2$, 3, and let $x^3 + ax + b$ (where $a, b \in K$) be a cubic polynomial with no multiple roots. An *elliptic*