

By the *projective plane* we mean the set of equivalence classes of triples  $(X, Y, Z)$  (not all components zero) where two triples are said to be equivalent if they are a scalar multiple of one another, i.e.,  $(\lambda X, \lambda Y, \lambda Z) \sim (X, Y, Z)$ . Such an equivalence class is called a *projective point*. If a projective point has nonzero  $Z$ , then there is one and only one triple in its equivalence class of the form  $(x, y, 1)$ : simply set  $x = X/Z$ ,  $y = Y/Z$ . Thus, the projective plane can be identified with all points  $(x, y)$  of the ordinary (“affine”) plane plus the points for which  $Z = 0$ . The latter points make up what is called the *line at infinity*; roughly speaking, it can be visualized as the “horizon” on the plane. Any equation  $F(x, y) = 0$  of a curve in the affine plane corresponds to an equation  $\tilde{F}(X, Y, Z) = 0$  satisfied by the corresponding projective points: simply replace  $x$  by  $X/Z$  and  $y$  by  $Y/Z$  and multiply by a power of  $Z$  to clear the denominators. For example, if we apply this procedure to the affine equation (1) of an elliptic curve, we obtain its “projective equation”  $Y^2Z = X^3 + aXZ^2 + bZ^3$ . This latter equation is satisfied by all projective points  $(X, Y, Z)$  with  $Z \neq 0$  for which the corresponding affine points  $(x, y)$ , where  $x = X/Z$ ,  $y = Y/Z$ , satisfy (1). In addition, what projective points  $(X, Y, Z)$  on the line at infinity satisfy the equation  $\tilde{F} = 0$ ? Setting  $Z = 0$  in the equation leads to  $0 = X^3$ , i.e.,  $X = 0$ . But the only equivalence class of triples  $(X, Y, Z)$  with both  $X$  and  $Z$  zero is the class of  $(0, 1, 0)$ . This is the point we call  $O$ . It is the point on the intersection of the  $y$ -axis with the line at infinity.

**Elliptic curves over the complexes.** The algebraic formulas (4)–(5) for adding points on an elliptic curve over the reals actually make sense over any field. (If the field has characteristic 2 or 3, one derives similar equations starting from Equation (2) or (3).) It can be shown that these formulas give an abelian group law on an elliptic curve over any field.

In particular, let  $E$  be an elliptic curve defined over the field  $\mathbf{C}$  of complex numbers. Thus,  $E$  is the set of pairs  $(x, y)$  of complex numbers satisfying Equation (1), together with the point at infinity  $O$ . Although  $E$  is a “curve,” if we think in terms of familiar geometrical pictures, it is 2-dimensional, i.e., it is a surface in the 4-real-dimensional space whose coordinates are the real and imaginary parts of  $x$  and  $y$ . We now describe how  $E$  can be visualized as a surface.

Let  $L$  be a *lattice* in the complex plane. This means that  $L$  is the abelian group of all integer combinations of two complex numbers  $\omega_1$  and  $\omega_2$  (where  $\omega_1$  and  $\omega_2$  span the plane, i.e., do not lie on the same line through the origin):  $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ . For example, if  $\omega_1 = 1$  and  $\omega_2 = i$ , then  $L$  is the Gaussian integers, the square grid consisting of all complex numbers with integer real and imaginary parts.

Given an elliptic curve (1) over the complex numbers, it turns out that there exist a lattice  $L$  and a complex function, called the “Weierstrass  $\wp$ -function” and denoted  $\wp_L(z)$ , which has the following properties.

1.  $\wp(z)$  is analytic except for a double pole at each point of  $L$ ;
2.  $\wp(z)$  satisfies the differential equation  $\wp'^2 = \wp^3 + a\wp + b$ , and hence for