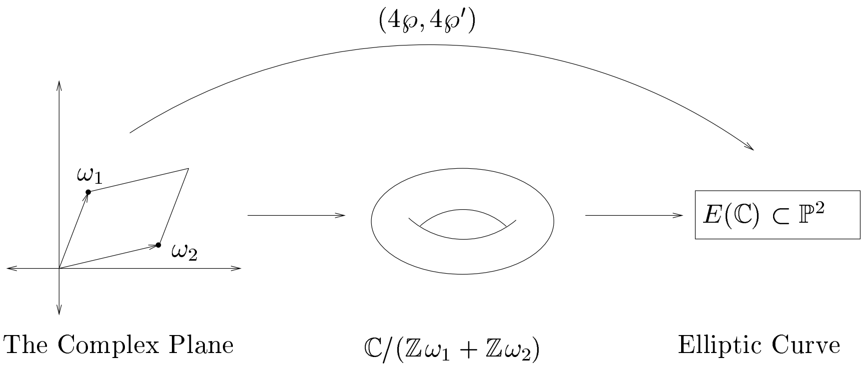

FIGURE 10.2. The Weierstrass $\wp$ Function and Elliptic Curves

10.2.5 Analytic Description of the Group Law

An alternative approach to the group law is via the Weierstrass $\wp$ function from complex analysis (see, e.g., [Ahl78,]). Let a and b be complex number with $4a^3 + 27b^2 \neq 0$. The Weierstrass $\wp$ function associated to a and b is a function $\wp : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ whose set of poles (points that map to ∞) are of the form $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where $\omega_1, \omega_2 \in \mathbb{C}$ have the property that $\mathbb{R}\omega_1 + \mathbb{R}\omega_2 = \mathbb{C}$. Note that the quotient $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ is homeomorphic to a torus. (In books, $\wp$ is usually viewed as being defined by $g_2 = -a/4$ and $g_3 = -b/16$.)

The connection with elliptic curves via $\wp$ is illustrated in Figure 10.2. If $x = 4\wp$ and $y = 4\wp'$, then $y^2 = x^3 + ax + b$, and $z \mapsto (4\wp(z), 4\wp'(z))$ extends to a complex analytic bijection

$$f : \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \to E(\mathbb{C}).$$

Since $\mathbb{C}/(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)$ is an abelian group, f induces a group structure on E. This group structure is the same as the one obtained above using divisors.

10.2.6 Geometric Description of the Group Law

Suppose $a, b \in \mathbb{R}$ and consider the elliptic curve defined by $y^2 = x^3+ax+b$. Since $a, b \in \mathbb{R}$ it makes sense to draw a graph of the subset

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b\} \subset E(\mathbb{C}).$$

Qualitatively, there are two possibilities for this picture, depending on whether $x^3 + ax + b$ has 1 or 3 real roots. If $x^3 + ax + b$ has 1 real root, then $R(\mathbb{R})$ looks like a bow, and if the cubic has 3 real roots, then $E(\mathbb{R})$ looks like the union of an egg and a bow. See Figure 10.3 for graphs of $y^2 = x^3 + 1$ (one real root) and $y^2 = x^3 - 5x + 4$ (three real roots).

Geometrically, the group law on $E(\mathbb{R})$ is defined as illustrated in Figure 10.4. To compute $P + Q$ draw the line L detetermined by $P + Q$ (if

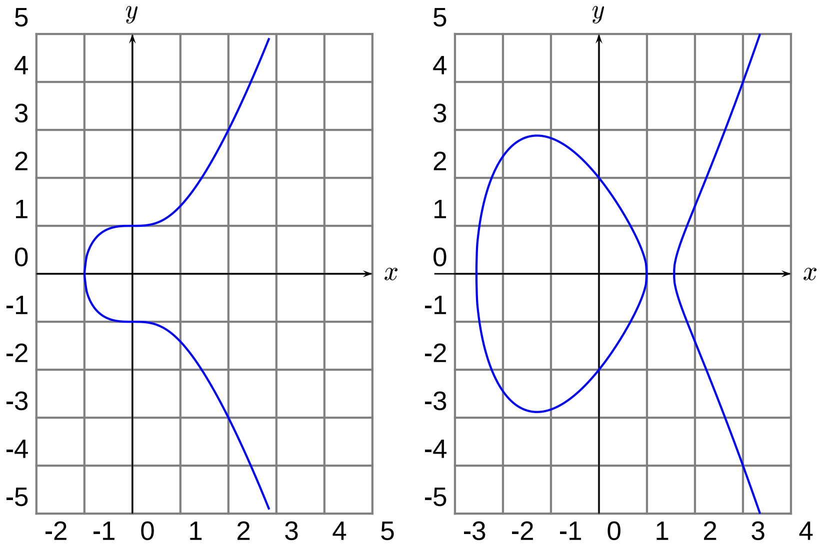

FIGURE 10.3. Real Points on $y^2 = x^3 + 1$ and $y^2 = x^3 - 5x + 4$

$P = Q$ let L be the tangent line to P). Let $R = (x, y)$ be the third point of intersection. Then the sum of $P + Q$ is $(x, -y)$. It is easy to see that the binary operation $E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R})$ determined by this process satisfies all the axioms of a group, except the associative law, which is much more tedious. (Note: One can rephrase all this geometry in a purely algebraic way, and then there is no need to restrict to real points.)

10.2.7 An Example

Let E be the elliptic curve defined by $y^2 = x^3 - 5x + 4$. Then $P = (0, 2)$, $Q = (1, 0)$, $R = (3, 4)$ and $R' = (3, -4)$ are elements of $E(\mathbb{C})$ and, as illustrated in Figure 10.4, $P + Q = R$. We verify this from the point of view of divisors and the Weierstrass $\wp$ function.

From the point of view of divisors, $P + Q = R$ is the assertion that

$$P - \mathcal{O} + Q - \mathcal{O} \sim R - \mathcal{O}.$$

To verify this, we exhibit a rational function f such that

$$(f) = P - \mathcal{O} + Q - \mathcal{O} - (R - \mathcal{O}) = P + Q - R - \mathcal{O},$$

i.e., so that f has simple zeros at P and Q and simples poles at R and $\mathcal{O}$. Let $f = \frac{2x+y-2}{x-3}$. Then

$$\begin{aligned}(2x + y - 2) &= P + Q + R' - 3\mathcal{O}\\ (x - 3) &= R + R' - 2\mathcal{O},\end{aligned}$$

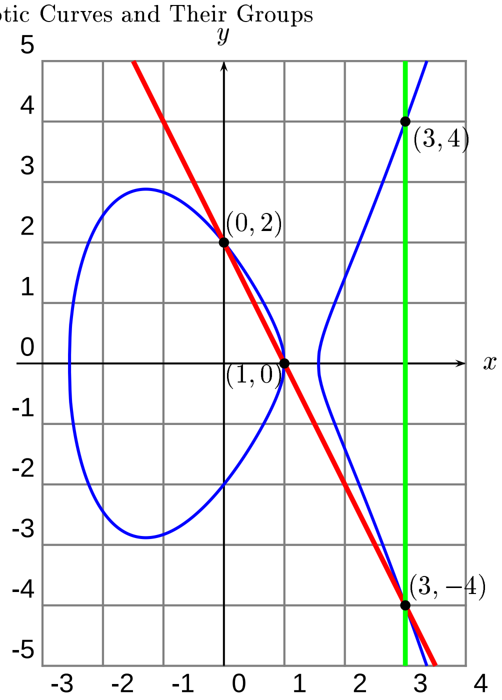

FIGURE 10.4. The Group Law: $(1,0)+(0,2)=(3,4)$ on $y^2=x^3-5x+4$

so

$$(f) = P + Q + R' - 3\mathcal{O} - (R + R' - 2\mathcal{O}) = P + Q - R - \mathcal{O}$$

as required.

Let $\wp$ be the Weierstrass function associated to $y^2 = x^3 - 5x + 4$. The poles of $\wp$ are the elements of $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where

$$\omega_1 = 2.39709803116447828 04\ldots, \quad \omega_2 = i1.60431066218451014 75\ldots.$$

Under the map $z \mapsto (4\wp(z), 4\wp'(z))$ we have

$$\begin{aligned} z_P &= 0.58916472693707629\ldots + i0.8021553310922550\ldots \mapsto P\\ z_Q &= 1.19854901558223914\ldots + i0.8021553310922588\ldots \mapsto Q\\ z_R &= 1.78771374251931543\ldots \mapsto R \end{aligned}$$

We have $z_P + z_Q = z_R + \omega_2$, so $z_P + z_Q = z_R \pmod{\Lambda}$, as expected.