as the inverse to the integral $\int dt/\sqrt{4t^3 - g_2 t - g_3}$. Weierstrass (1863), p. 121, found the relations between g_2, g_3 and the periods ω_1, ω_2:

$$g_2 = 60\sum \frac{1}{(m\omega_1 + n\omega_2)^4},$$

$$g_3 = 140\sum \frac{1}{(m\omega_1 + n\omega_2)^6},$$

where the sums are over all pairs $(m,n) \neq (0,0)$. Elegant modern accounts of the Eisenstein and Weierstrass theories may be found in Weil (1976) and Robert (1973).

Exercises

The precise definition of the Weierstrass $\wp$-function is

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n\neq 0,0}^{\infty} \left(\frac{1}{(z + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right).$$

This series has better convergence than the Eisenstein series given above, but its double periodicity is not quite so obvious. We can establish double periodicity by differentiating and integrating as follows (which is valid because of the convergence properties of the Weierstrass series).

16.4.1 By differentiating term by term, show that

$$\wp'(z) = -2 \sum_{m,n=-\infty}^{\infty} \frac{1}{(z + m\omega_1 + n\omega_2)^3},$$

and conclude that $\wp'(z+\omega_1) = \wp'(z)$ and $\wp'(z+\omega_2) = \wp'(z)$.

16.4.2 By integrating the equations just obtained, show that

$$\wp(z+\omega_1) - \wp(z) = c \quad \text{and} \quad \wp(z+\omega_2) - \wp(z) = d,$$

for some constants c and d.

16.4.3 Deduce from Exercise 16.4.2 that

$$\wp\left(\frac{\omega_1}{2}\right) - \wp\left(-\frac{\omega_1}{2}\right) = c \quad \text{and} \quad \wp\left(\frac{\omega_2}{2}\right) - \wp\left(-\frac{\omega_2}{2}\right) = d.$$

16.4.4 But $\wp(z) = \wp(-z)$ (why?); hence conclude that $\wp$ is doubly periodic.

16.5 Elliptic Curves

We have seen that nonsingular cubic curves of the form

$$y^2 = ax^3 + bx^2 + cx + d \tag{1}$$

are important not only among the cubic curves themselves (see Newton's classification, Sections 7.4 and 8.4), but also in number theory (Section 11.6) and the theory of elliptic functions (Section 12.2). One of the great achievements of nineteenth-century mathematics was the synthesis of a unified view of all these manifestations of cubic curves. The view was first glimpsed by Jacobi (1834), and it came more clearly into focus with the development of complex analysis between Riemann (1851) and Poincaré (1901). The theory of elliptic curves, as the unified view has come to be known, continues to inspire researchers today, as it seems to encompass some of the most fascinating problems of number theory. We now know, for example, how to derive Fermat's last theorem from properties of elliptic curves (see Section 11.3).

Jacobi saw, at least implicitly, that the curve (1) could be parameterized as

$$x = f(z), \qquad y = f'(z), \tag{2}$$

where f and its derivative f' are elliptic functions. Knowing that f and f' were doubly periodic, with the same periods ω_1, ω_2, say, he would have seen that this gave a map of the z plane $\mathbb{C}$ onto the curve (1) for which the preimage of a given point on (1) is a set of points in $\mathbb{C}$ of the form

$$z + \Lambda = \{z + m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\},$$

where

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$$

is called the *lattice of periods* of f. The numbers $z + m\omega_1 + n\omega_2$ in $z + \Lambda$ are also called "equivalent with respect to Λ." One such equivalence class is shown by asterisks in Figure 16.2.

The parameterization (2) means that there is a one-to-one correspondence between the points $(f(z), f'(z))$ of the curve and the equivalence classes $z + \Lambda$. Today we express this relation by saying that the curve is *isomorphic to the space* $\mathbb{C}/\Lambda$ of these equivalence classes. Jacobi might have seen, though it was probably not of interest to him, that $\mathbb{C}/\Lambda$ is a torus. One sees this by taking one parallelogram in $\mathbb{C}$, which includes

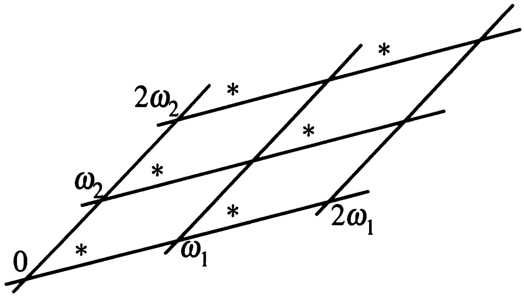

Figure 16.2: Lattice-equivalent points

a representative of each equivalence class, and identifying the equivalent points on its boundary (that is, pasting opposite sides together, as in Figure 16.3). Of course, the torus form of (1) eventually came to light through the Riemann surface construction given in Section 15.4.

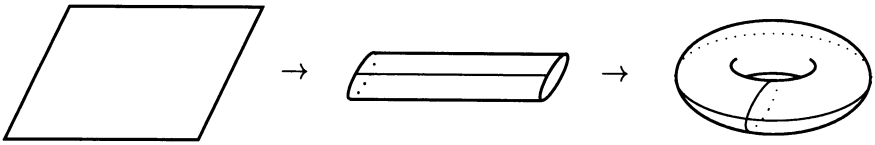

Figure 16.3: Construction of a torus by pasting

An elegant way of demonstrating both the double periodicity of elliptic functions and the parameterization of cubic curves was given by Weierstrass (1863). Beginning with the function

$$\sum_{m,n=-\infty}^{\infty} \frac{1}{(z+m\omega_1+n\omega_2)^2},$$

which, as mentioned in Section 16.4, makes the double periodicity evident, Weierstrass defined the function

$$\wp(z) = \frac{1}{z^2} + \sum_{m,n\neq 0,0}^{\infty} \left(\frac{1}{(z+m\omega_1+n\omega_2)^2} - \frac{1}{(m\omega_1+n\omega_2)^2} \right),$$

which has better convergence properties and is also doubly periodic. He then showed by simple computations with series that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where g_2, g_3 are the constants depending on ω_1, ω_2, which were defined in Section 16.4. It follows that the point $(\wp(z), \wp'(z))$ lies on the curve

$$y^2 = 4x^3 - g_2 x - g_3, \tag{3}$$

and a little further checking shows that (3) is in fact isomorphic to $\mathbb{C}/\Lambda$, where Λ is the lattice of periods of $\wp$. The parameterization of all curves (1) by elliptic functions follows by making a linear transformation.

Once the curve (1) is parameterized as

$$x = f(z), \qquad y = f'(z),$$

one sees a natural "addition" of points on the curve induced by adding their parameter values. Because of the double periodicity of f and f', this "addition" is simply ordinary addition in $\mathbb{C}$, modulo Λ. In particular, it is immediate that "addition of points" has some properties of ordinary addition, such as commutativity and associativity. However, as mentioned in Section 11.6, addition of parameter values z is also reflected in the geometry of the curve. The most concise statement of the relationship, due to Clebsch (1864), is that if z_1, z_2, z_3 are parameter values of three collinear points, then

$$z_1 + z_2 + z_3 = 0 \mod (\omega_1, \omega_2)$$

(or $z_1 + z_2 + z_3 \in \Lambda$). This means that "addition of points" also has an elementary geometric interpretation, for which, incidentally, the algebraic properties are far less obvious.

On the other hand, the straight-line interpretation of "addition" gives the simplest explanation of the addition theorems for elliptic functions. As we saw in Section 11.6, the value of $f(z_3)$ is easy to compute as a rational function of $f(z_1)$, $f'(z_1)$, $f(z_2)$, $f'(z_2)$ when z_1, z_2, z_3 are the parameter values of collinear points. Originally, of course, the formula was obtained by Euler, with great difficulty, by manipulating the integral inverse to f (see Section 12.5).

Another reason to accept $\mathbb{C}/\Lambda$ as the "right" view of the curve is that it gives an answer to the seemingly unrelated question of classification by projective equivalence. Recall from Section 8.4 that Newton had reduced cubics to the cusp type, the double-point type, and three nonsingular types using real projective transformations. All cubics with a cusp are, in fact, equivalent to $y^2 = x^3$, and all with a double point are equivalent to $y^2 = x^2(x+1)$, while the distinction between the nonsingular types disappears over the complex numbers, where, as we now know, all are equivalent to tori $\mathbb{C}/\Lambda$. The problem that remains is to decide projective equivalence among the nonsingular cubics. Salmon (1851) showed that this was determined by a certain complex number τ, which could be computed from the equation of the curve. He defined τ geometrically, so that its projective invariance was obvious, with no thought of elliptic functions. But τ turned out to be nothing but ω_1/ω_2, which means that two nonsingular cubics are projectively equivalent if and only if their period lattices Λ have the same shape.

EXERCISES

Strictly speaking, the ratio $\tau = \omega_1/\omega_2$ determines only the shape of the *parallelogram* with vertices 0, ω_1, ω_2, and $\omega_1 + \omega_2$.

16.5.1 Explain how both the angle between adjacent sides of this parallelogram, and the ratio between their lengths, may be extracted from $\tau = \omega_1/\omega_2$.

The lattice of periods

$$\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$$

can be viewed as the set of vertices in a tiling of the plane by copies of this parallelogram, as in Figure 16.2. However, infinitely many *differently shaped parallelograms* give the same Λ. Thus the number τ alone should not be taken to characterize the shape of Λ.

16.5.2 Show that Λ may also be tiled by copies of a parallelogram with shape given by $\tau + 1$.

16.5.3 More generally, show that Λ may be generated by any two of its elements, $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$ provided $ad - bc = \pm 1$. *Hint*: Write down a product of matrices transforming the column vector of (ω_1, ω_2) to (ω_1', ω_2') and back to (ω_1, ω_2), and take its determinant.

16.5.4 Deduce from Exercise 16.5.3 that the lattice $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$ has shape characterized by the whole family of complex numbers

$$\frac{a\tau + b}{c\tau + d} \quad \text{where} \quad \tau = \frac{\omega_1}{\omega_2} \quad \text{and} \quad a, b, c, d \text{ are integers with } ad - bc = \pm 1.$$

There are functions of the complex variable τ that depend only on the lattice Λ, and hence take the same value for each number $(a\tau + b)/(c\tau + d)$ characterizing the lattice shape.

16.5.5 Consider g_2 and g_3 from Section 16.4, which are obviously functions $g_2(\Lambda)$ and $g_3(\Lambda)$ of the lattice Λ. Show that g_2^3/g_3^2 and $g_2^3/(g_2^3 - 27g_3^2)$ are both functions of τ.

The latter function is none other than the famous *modular function* mentioned in Section 6.7 in connection with the solution of the quintic equation. For more information on its amazing properties, see McKean and Moll (1997).

16.6 Uniformization

The characteristic of nonsingular cubics that allows their parameterization by elliptic functions is their topological form. The two periods correspond to the two essentially different circuits around the torus (Figure 16.1).

A representation of the x and y values on a curve by simultaneous functions of a single parameter z is sometimes called a *uniform* representation, and so the problem of parameterizing all algebraic curves in this way came to be known as the *uniformization* problem. Once the elliptic case was understood, it became clear that a solution of the uniformization problem for arbitrary algebraic curves would depend on a better understanding of surfaces: their topology, the periodicities associated with their closed curves, and the way these periodicities could be reflected in $\mathbb{C}$. These problems were first attacked by Poincaré and Klein in the 1880s, and their work led to the eventual positive solution of the uniformization problem by Poincaré (1907) and Koebe (1907).

Even more important than the solution of this single problem, however, was the amazing convergence of ideas in the preliminary work of Poincaré and Klein. They discovered that multiple periodicities were reflected in $\mathbb{C}$ by groups of transformations, and that the transformations in question were of the simple type $z \mapsto (az+b)/(cz+d)$, called *linear fractional*. Linear fractional transformations generalize the linear transformations $z \mapsto z+\omega_1$, $z \mapsto z+\omega_2$ naturally associated with the periods of elliptic functions. However, while the transformations $z \mapsto z+\omega_1$, $z \mapsto z+\omega_2$ are algebraically and geometrically transparent—they commute, and they generate the general transformations $z \mapsto z+m\omega_1+n\omega_2$, which are simply translations of the plane—the more general linear fractional transformations are not as easily understood. Linear fractional transformations do not normally commute, and their mastery requires a simultaneous grasp of algebraic, geometric, and topological aspects.

The simultaneous view proved to be enormously fruitful in the development of group theory and topology, as we shall see in Chapters 19 and 22. Geometry was also given a new lease of life when Poincaré (1882) discovered that linear fractional transformations give a natural interpretation of noneuclidean geometry, a field which until then had been a curiosity on the fringes of mathematics. In the next two chapters we look at the origins of noneuclidean geometry and see how the subject was transformed by Poincaré's discovery.

EXERCISES

The first example, beyond the elliptic functions, of periodicity under linear fractional transformations is seen in the modular function derived in the previous exercise set. It turns out that the periodicity of the modular function can be generated by two transformations: $z \mapsto z+1$ and $z \mapsto -1/z$.

16.6.1 Check that $z \mapsto z+1$ and $z \mapsto -1/z$ are among the transformations

$$z \mapsto \frac{az+b}{cz+d} \quad \text{where } a,b,c,d \text{ are integers with } ad-bc = \pm 1.$$

16.6.2 Show that the transformations $z \mapsto z+1$ and $z \mapsto -1/z$ do not commute.

16.6.3 Show that both $z \mapsto z+1$ and $z \mapsto -1/z$ map the half-plane $\{\operatorname{Im} z > 0\}$ onto itself, and that $z \mapsto -1/z$ exchanges the inside and outside of the unit circle.

16.7 Biographical Notes: Lagrange and Cauchy

Joseph Louis Lagrange (Figure 16.4) was born in Turin in 1736 and died in Paris in 1813. He was the oldest of 11 children of Guiseppe Lagrangia, treasurer of the Office of Public Works in Turin, and Teresa Grosso, the daughter of a physician, and a member of the wealthy Conti family. Despite this background, Lagrange's family was not well off, as his father had made some unwise financial speculations. Lagrange eventually came to appreciate the loss of his chance to become a wealthy idler, saying, "If I had inherited a fortune I should probably not have cast my lot with mathematics."

His prowess in mathematics developed with amazing speed after he first encountered calculus in 1753, at the age of 17. By 1754 he was writing to Euler about his discoveries, and in 1755 he was made professor at the Royal Artillery School in Turin. As early as 1756 he was offered a superior position in Prussia, but he was too shy, or too reluctant to leave home, to accept it. As his reputation grew, he also won the support of d'Alembert. When Euler left Berlin in 1766, d'Alembert arranged for Lagrange to take Euler's place. In 1767, perhaps missing the company of his family in Turin,

Figure 16.4: Joseph Louis Lagrange

Lagrange married his cousin Vittoria Conti. In a letter to d'Alembert in 1769 he said he had chosen a wife "who is one of my good cousins and who even lived for a long time with my family, is a very good housewife and has no pretensions at all," adding that they had no children and did not want any.

Notwithstanding this lackluster beginning, and the ill health of both Lagrange and his wife, the marriage strengthened over the years. Lagrange nursed Vittoria as her health worsened, and he was heartbroken when she died in 1783. He became deeply depressed about his work and the future of mathematics itself, writing to d'Alembert: "I cannot say that I shall still be doing mathematics 10 years from now. It also seems to me that the mine is already too deep, and that unless new veins are discovered it will have to be abandoned." Not long before this, Lagrange had completed one of his greatest works, the *Mécanique analytique*, but when a copy of the book reached him from the printer he left it unopened on his desk.

Frederick II died in 1786, and Lagrange's position in Berlin became