Problem 11 so as to get the other values of z for which $u = \wp(z)$, namely $\pm z + m\omega_1 + n\omega_2$.

13. Suppose that $g_2 = 4n^2$, $g_3 = 0$. Take e_1, e_2, e_3 so that $e_2 > e_3 > e_1$. What are e_1, e_2, e_3 in this case? Show that $\omega_1 = i\omega_2$, i.e., the lattice L is the Gaussian integer lattice expanded by a factor of ω_2. Show that as z travels along the straight line from $\omega_1/2$ to $\omega_1/2 + \omega_2$ the point $(x, y) = (\wp(z), \wp'(z))$ moves around the real points of the elliptic curve $y^2 = 4(x^3 - n^2x)$ between $-n$ and 0; and as z travels along the straight line from 0 to ω_2 the point $(x, y) = (\wp(z), \wp'(z))$ travels through all the real points of this elliptic curve which are to the right of $(n, 0)$. Think of the "open" appearance of the latter path to be an optical illusion: the two ends are really "tied together" at the point at infinity $(0, 1, 0)$.

14. (a) Show that $\displaystyle\int_0^1 \frac{t^n dt}{\sqrt{t(1-t)}} = \frac{\pi}{n!}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdots\left(n-\frac{1}{2}\right)$ for $n = 0, 1, 2, \ldots$.

(b) Under the conditions of Problem 12, with $e_2 > e_3 > e_1$, set $\lambda = \dfrac{e_3 - e_1}{e_2 - e_1} \in (0, 1)$. Derive the formula:

$$\omega_2 = \frac{1}{\sqrt{e_2 - e_1}} \int_0^1 \frac{dt}{\sqrt{t(1-t)(1-\lambda t)}}.$$

(c) Derive the formula $\omega_2 = \pi(e_2 - e_1)^{-1/2} F(\lambda)$, where

$$F(\lambda) = \sum_{n=0}^{\infty} \left[\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdots\left(n-\frac{1}{2}\right)\right]^2 \frac{\lambda^n}{n!^2}.$$

The function $F(\lambda)$ is called a "hypergeometric series".

(d) Show that the hypergeometric series in part (c) satisfies the differential equation: $\lambda(1-\lambda)F''(\lambda) + (1-2\lambda)F'(\lambda) - \frac{1}{4}F(\lambda) = 0$.

§7. The addition law

In the last section we showed how the Weierstrass $\wp$-function gives a correspondence between the points of $\mathbb{C}/L$ and the points on the elliptic curve $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$ in $\mathbb{P}^2_{\mathbb{C}}$. We have an obvious addition law for points in $\mathbb{C}/L$, obtained from ordinary addition of complex numbers by dividing by the additive subgroup L, i.e., ordinary addition "modulo L". This is the two-dimensional analog of "addition modulo one" in the group $\mathbb{R}/\mathbb{Z}$.

We can use the correspondence between $\mathbb{C}/L$ and the elliptic curve to carry over the addition law to the points on the elliptic curve. That is, to add two points $P_1(x_1, y_1)$ and $P_2 = (x_2, y_2)$, by definition what we do is go back to the z-plane, find z_1 and z_2 such that $P_1 = (\wp(z_1), \wp'(z_1))$ and $P_2 = (\wp(z_2), \wp'(z_2))$, and then set $P_1 + P_2 = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$. This is just a case of the general principle: whenever we have a one-to-one correspondence between elements of a commutative group and elements of some

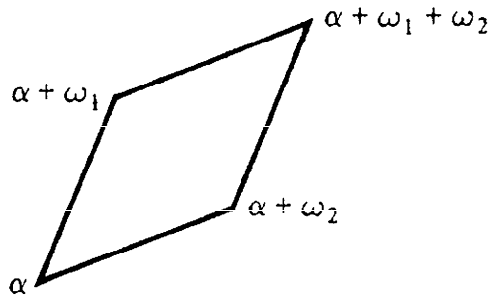

Figure I.12

other set, we can use this correspondence to define a commutative group law on that other set.

But the remarkable thing about the addition law we obtain in this way is that (1) there is a simple geometric interpretation of "adding" the points on the elliptic curve, and (2) the coordinates of $P_1 + P_2$ can be expressed directly in terms of x_1, x_2, y_1, y_2 by rather simple rational functions. The purpose of this section is to show how this is done.

We first prove a general lemma about elliptic functions.

Lemma. *Let $f(z) \in \mathscr{E}_L$. Let $\Pi = \{a\omega_1 + b\omega_2 | 0 \le a, b \le 1\}$ be a fundamental parallelogram for the lattice L, and choose α so that $f(z)$ has no zeros or poles on the boundary of $\alpha + \Pi$. Let $\{a_i\}$ be the zeros of $f(z)$ in $\alpha + \Pi$, each repeated as many times as its multiplicity, and let $\{b_j\}$ be the poles, each occurring as many times as its multiplicity. Then $\Sigma a_i - \Sigma b_j \in L$.*

PROOF. Recall that the function $f'(z)/f(z)$ has poles at the zeros and poles of $f(z)$, and its expansion near a zero a of order m is $m/(z-a) + \cdots$ (and near a pole b of order $-m$ the expansion is $-m/(z-b) + \cdots$). Then the function $zf'(z)/f(z)$ has the same poles, but, writing $z = a + (z-a)$, we see that the expansion starts out $am/(z-a)$. We conclude that $\Sigma a_i - \Sigma b_j$ is the sum of the residues of $zf'(z)/f(z)$ inside $\alpha + \Pi$. Let C be the boundary of $\alpha + \Pi$. By the residue theorem,

$$\sum a_i - \sum b_j = \frac{1}{2\pi i} \int_C \frac{zf'(z)}{f(z)} dz.$$

We first take the integral over the pair of opposite sides from α to $\alpha + \omega_2$ and from $\alpha + \omega_1$ to $\alpha + \omega_1 + \omega_2$ (see Fig. I.12). This part is equal to

$$\begin{aligned}
&\frac{1}{2\pi i}\left(\int_\alpha^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz\right) \\
&\quad = \frac{1}{2\pi i}\left(\int_\alpha^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_\alpha^{\alpha+\omega_2} (z+\omega_1)\frac{f'(z)}{f(z)}dz\right) \\
&\quad = -\omega_1 \frac{1}{2\pi i}\int_\gamma^{\alpha+\omega_2} \frac{f'(z)}{f(z)}dz.
\end{aligned}$$

Now make the change of variables $u = f(z)$, so that $f'(z)dz/f(z) = du/u$. Let C_1 be the closed path from $f(\alpha)$ to $f(\alpha + \omega_2) = f(\alpha)$ traced by $u = f(z)$ as z goes from α to $\alpha + \omega_2$. Then

$$\frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{C_1}\frac{du}{u},$$

and this is some integer n, namely the number of times the closed path C_1 winds around the origin (counterclockwise). Thus, we obtain $-\omega_1 n$ for this part of our original integral. In the same way, we find that the integral over the remaining two sides of C is equal to $-\omega_2 m$ for some integer m. Thus, $\Sigma a_i - \Sigma b_j = -n\omega_1 - m\omega_2 \in L$, as desired. This proves the lemma. □

We are now ready to derive the geometrical procedure for adding two points on the elliptic curve $y^2 = f(x) = x^3 - g_2(L)x - g_3(L)$. For z in $\mathbb{C}/L$, let P_z be the corresponding point $P_z = (\wp(z), \wp'(z), 1)$, $P_0 = (0, 1, 0)$ on the elliptic curve. Suppose we want to add $P_{z_1} = (x_1, y_1)$ to $P_{z_2} = (x_2, y_2)$ to obtain the sum $P_{z_1+z_2} = (x_3, y_3)$. We would like to know how to go from the two points to their sum directly, without tracing the points back to the z-plane.

We first treat some special cases. The additive identity is, of course, the image of $z = 0$. Let 0 denote the point at infinity (0, 1, 0), i.e., the additive identity of our group of points. The addition is trivial if one of the points is 0, i.e., if z_1 or z_2 is zero. Next, suppose that P_{z_1} and P_{z_2} have the same x-coordinate but are not the same point. This means that $x_2 = x_1, y_2 = -y_1$. In this case $z_2 = -z_1$, because only "symmetric" values of z (values which are the negatives of each other modulo the lattice L) can have the same $\wp$-value. In this case, $P_{z_1} + P_{z_2} = P_0 = 0$, i.e., the two points are additive inverse to one another. Speaking geometrically, we say that two points of the curve which are on the same vertical line have sum 0. We further note that in the special situation of a point $P_{z_1} = P_{z_2}$ on the x-axis, we have $y_2 = -y_1 = 0$, and it is easy to check that we still have $P_{z_1} + P_{z_2} = 2P_{z_1} = 0$. We have proved:

Proposition 11. *The additive inverse of* (x, y) *is* $(x, -y)$.

Given two points $P_1 = P_{z_1} = (x_1, y_1)$ and $P_2 = P_{z_2} = (x_2, y_2)$ on the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ (neither the point at infinity 0), there is a line $l = \overline{P_1P_2}$ joining them. If $P_1 = P_2$, we take l to be the tangent line to the elliptic curve at P_1. If l is a vertical line, then we saw that $P_1 + P_2 = 0$. Suppose that l is not a vertical line, and we want to find $P_1 + P_2 = P_3 = (x_3, y_3)$. Our basic claim is that $-P_3 = (x_3, -y_3)$ is the third point of intersection of the elliptic curve with l.

Write the equation of $l = \overline{P_1P_2}$ in the form $y = mx + b$. A point (x, y) on l is on the elliptic curve if and only if $(mx + b)^2 = f(x) = 4x^3 - g_2x - g_3$, that is, if and only if x is a root of the cubic $f(x) - (mx + b)^2$. This cubic

has three roots, each of which gives a point of intersection. If x is a double root or triple root, then l intersects the curve with multiplicity two or three at the point (x, y) (see Problem 6 of §I.3). In any case, the total number of points of intersection (counting multiplicity) is three.

Notice that vertical lines also intersect the curve in three points, including the point at infinity 0; and the line at infinity has a triple intersection at 0 (see Problem 7 of §I.3). Thus, any line in $\mathbb{P}^2_{\mathbb{C}}$ intersects the curve in three points. This is a special case of

Bezout's Theorem. *Let $\tilde{F}(x, y, z)$ and $\tilde{G}(x, y, z)$ be homogeneous polynomials of degree m and n, respectively, over an algebraically closed field K. Suppose that $\tilde{F}$ and $\tilde{G}$ have no common polynomial factor. Then the curves in $\mathbb{P}^2_K$ defined by $\tilde{F}$ and $\tilde{G}$ have mn points of intersection, counting multiplicities.*

For a more detailed discussion of multiplicity of intersection and a proof of Bezout's theorem, see, for example, Walker's book an algebraic curves [Walker 1978].

In our case $\tilde{F}(x, y, z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3$ and $\tilde{G}(x, y, z) = y - mx - bz$.

Proposition 12. *If $P_1 + P_2 = P_3$, then $-P_3$ is the third point of intersection of $l = \overline{P_1P_2}$ with the elliptic curve. If $P_1 = P_2$, then by $\overline{P_1P_2}$ we mean the tangent line at P_1.*

PROOF. We have already treated the case when P_1 or P_2 is the point at infinity 0, and when $P_2 = -P_1$. So suppose that $l = \overline{P_1P_2}$ has the form $y = mx + b$. Let $P_1 = P_{z_1}$, $P_2 = P_{z_2}$. To say that a point $P_z = (\wp(z), \wp'(z))$ is on l means that $\wp'(z) = m\wp(z) + b$. The elliptic function $\wp'(z) - m\wp(z) - b$ has three poles and hence three zeros in $\mathbb{C}/L$. Both z_1 and z_2 are zeros. According to the lemma proved above, the sum of the three zeros and three poles is equal to zero modulo the lattice L. But the three poles are all at zero (where $\wp'(z)$ has a triple pole); thus, the third zero is $-(z_1 + z_2)$ modulo the lattice. Hence, the third point of intersection of l with the curve is $P_{-(z_1+z_2)} = -P_{z_3}$, as claimed.

The argument in the last paragraph is rigorous only if the three points of intersection of l with the elliptic curve are distinct, in which case a zero of $\wp'(z) - m\wp(z) - b$ corresponds exactly to a point of intersection P_z. Otherwise, we must show that a double or triple zero of the elliptic function always corresponds to a double or triple intersection, respectively, of l with the curve. That is, we must show that the two meanings of the term "multiplicity" agree: multiplicity of zero of the elliptic function of the variable z, and multiplicity of intersection in the xy-plane.

Let z_1, z_2, $-z_3$ be the three zeros of $\wp'(z) - m\wp(z) - b$, listed as many times as their multiplicity. Note that none of these three points is the negative of another one, since l is not a vertical line. Since $-z_1$, $-z_2$, z_3 are the three

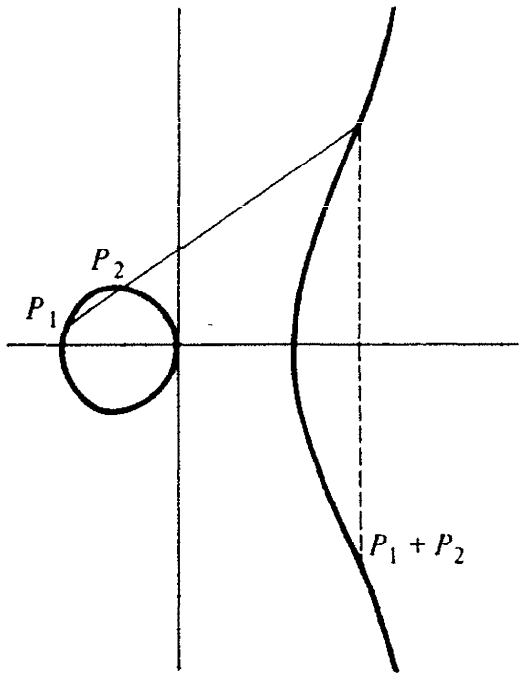

Figure I.13

zeros of $\wp'(z) + m\wp(z) + b$, it follows that $\pm z_1$, $\pm z_2$, $\pm z_3$ are the six zeros of $\wp'(z)^2 - (m\wp(z) + b)^2 = f(\wp(z)) - (m\wp(z) + b)^2 = 4(\wp(z) - x_1)(\wp(z) - x_2)(\wp(z) - x_3)$, where x_1, x_2, x_3 are the roots of $f(x) - (mx + b)^2$. If, say, $\wp(z_1) = x_1$, then the multiplicity of x_1 depends upon the number of $\pm z_2$, $\pm z_3$ which equal $\pm z_1$. But this is precisely the number of z_2, $-z_3$ which equal z_1. Hence "multiplicity" has the same meaning in both cases.

This concludes the proof of Proposition 12. □

Proposition 12 gives us Fig. I.13, which illustrates the group of real points on the elliptic curve $y^2 = x^3 - x$. To add two points P_1 and P_2, we draw the line joining them, find the third point of intersection of that line with the curve, and then take the symmetric point on the other side of the x-axis.

It would have been possible to define the group law in this geometrical manner in the first place, and prove directly that the axioms of an abelian group are satisfied. The hardest part would have been the associative law, which would have necessitated a deeper investigation of intersections of curves. In turns out that there is some flexibility in defining the group law. For example, any one of the eight points of inflection besides the point at infinity could equally well have been chosen as the identity. For details of this alternate approach, see [Walker 1978].

One disadvantage of our approach using $\wp(z)$ is that *a priori* it only applies to elliptic curves of the form $y^2 = 4x^3 - g_2(L)x - g_3(L)$ or curves that can be transformed to that form by a linear change of variables. (Note that the geometrical description of the group law will still give an abelian group law after a linear change of variables.) In actual fact, as was mentioned earlier and will be proved later, any elliptic curve over the complex numbers can be transformed to the Weierstrass form for some lattice L. We already know

that our favorite example $y^2 = x^3 - n^2x$ corresponds to a multiple of the Gaussian integer lattice. In the exercises for this section and the next, we shall allow ourselves to use the fact that the group law works for any elliptic curve.

It is not hard to translate this geometrical procedure into formulas expressing the coordinates (x_3, y_3) of the sum of $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in terms of x_1, x_2, y_1, y_2 and the coefficients of the equation of the elliptic curve. Although, strictly speaking, our derivation was for elliptic curves in the form $y^2 = f(x) = 4x^3 - g_2(L)x - g_3(L)$ for some lattice L, the procedure gives an abelian group law for any elliptic curve $y^2 = f(x)$, as remarked above. So let us take $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ to be any cubic with distinct roots.

In what follows, we shall assume that neither P_1 nor P_2 is the point at infinity 0, and that $P_1 \neq -P_2$. Then the line through P_1 and P_2 (the tangent line at P_1 if $P_1 = P_2$) can be written in the form $y = mx + \beta$, where $m = (y_2 - y_1)/(x_2 - x_1)$ if $P_1 \neq P_2$ and $m = dy/dx|_{(x_1, y_1)}$ if $P_1 = P_2$. In the latter case we can express m in terms of x_1 and y_1 by implicitly differentiating $y^2 = f(x)$; we find that $m = f'(x_1)/2y_1$. In both cases the y-intercept is $\beta = y_1 - mx_1$.

Then x_3, the x-coordinate of the sum, is the third root of the cubic $f(x) - (mx + \beta)^2$, two of whose roots are x_1, x_2. Since the sum of the three roots is equal to minus the coefficient of x^2 divided by the leading coefficient, we have: $x_1 + x_2 + x_3 = -(b - m^2)/a$, and hence:

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \qquad \text{if} \quad P_1 \neq P_2; \tag{7.1}$$

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2, \qquad \text{if} \quad P_1 = P_2. \tag{7.2}$$

The y-coordinate y_3 is the negative of the value $y = mx_3 + \beta$, i.e.,

$$y_3 = -y_1 + m(x_1 - x_3), \tag{7.3}$$

where x_3 is given by (7.1) and (7.2), and

$$\begin{aligned} m &= (y_2 - y_1)/(x_2 - x_1) \quad \text{if} \quad P_1 \neq P_2; \\ m &= f'(x_1)/2y_1 \qquad\qquad \text{if} \quad P_1 = P_2. \end{aligned} \tag{7.4}$$

If our elliptic curve is in Weierstrass form $y^2 = 4x^3 - g_2x - g_3$, then we have $a = 4$, $b = 0$, and $f'(x_1) = 12x_1^2 - g_2$ in the addition formulas (7.1)–(7.4).

In principle, we could have simply defined the group law by means of these formulas, and then verified algebraically that the axioms of a commutative group are satisfied. The hardest axiom to verify would be associativity. Tedious as this procedure would be, it would h ıe key advantage over

either the complex-analytic procedure (using $\wp(z)$) or the geometrical procedure. Namely, we would never have to use the fact that our field K over which the elliptic curve is defined is the complex numbers, or even that it has characteristic zero. That is, we would find that our formulas, which make sense over any field K of characteristic not equal to 2, give an abelian group law. That is, if $y^2 = f(x) = ax^3 + bx^2 + cx + d \in K[x]$ is the equation of an elliptic curve over K, and if we define $f'(x) = 3ax^2 + 2bx + c$, then any two points having coordinates in some extension of K can be added using the formulas (7.1)–(7.4). We shall make use of this fact in what follows, even though, strictly speaking, we have not gone through the tedious purely algebraic verification of the group laws.

Problems

1. Let $L \subset \mathbb{R}$ be the additive subgroup $\{m\omega\}$ of multiples of a fixed nonzero real number ω. Then the function $z \mapsto (\cos(2\pi z/\omega), \sin(2\pi z/\omega))$ gives a one-to-one analytic map of $\mathbb{R}/L$ onto the curve $x^2 + y^2 = 1$ in the real xy-plane. Show that ordinary addition in $\mathbb{R}/L$ carries over to a rational (actually polynomial) law for "adding" two points (x_1, y_1) and (x_2, y_2) on the unit circle; that is, the coordinates of the "sum" are polynomials in x_1, x_2, y_1, y_2. Thus, the rational addition law on an elliptic curve can be thought of as a generalization of the formulas for the sine and cosine of the sum of two angles.

2. (a) Simplify the expression for the x-coordinate of $2P$ in the case of the elliptic curve $y^2 = x^3 - n^2x$.
   (b) Let X, Y, Z be a rational right triangle with area n. Let P be the corresponding point on the curve $y^2 = x^3 - n^2x$ constructed in the text in §I.2. Let Q be the point constructed in Problem 2 of §I.2. Show that $P = 2Q$.
   (c) Prove that, if P is a point not of order 2 with rational coordinates on the curve $y^2 = x^3 - n^2x$, then the x-coordinate of $2P$ is the square of a rational number having even denominator. For example, the point $Q = ((41/7)^2, 720 \cdot 41/7^3)$ on the curve $y^2 = x^3 - 31^2x$ is not equal to twice a point P having rational coordinates. (In this problem, recall: n is always squarefree.)

3. Describe geometrically: (a) the four points of order two on an elliptic curve; (b) the nine points of order three; (c) how to find the twelve points of order four which are not of order two; (d) what the associative law of addition says about a certain configuration of lines joining points on the elliptic curve (draw a picture).

4. (a) How many points of inflection are there on an elliptic curve besides the point at infinity? Notice that they occur in symmetric pairs. Find an equation for their x-coordinates.
   (b) In the case of the elliptic curve $y^2 = x^3 - n^2x$ find an explicit formula for these x-coordinates. Show that they are never rational (for any n).

5. Given a point Q on an elliptic curve, how many points P are there such that $2P = Q$? Describe geometrically how to find them.

6. Show that if K is any subfield of $\mathbb{C}$ containing g_2 and g_3, then the points on the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ whose coordinates are in K form a subgroup