§6. Elliptic curves in Weierstrass form

As remarked at the end of the last section, from the proof of Proposition 9 we can immediately conclude that the square of $\wp'(z)$ is equal to a cubic polynomial in $\wp(z)$. More precisely, we know that $\wp'(z)^2$ has a double zero at $\omega_1/2$, $\omega_2/2$, and $(\omega_1+\omega_2)/2$ (see Problem 4 of §5). Hence, these three numbers are the a_i's, and we have

$$\begin{aligned}\wp'(z)^2 &= C(\wp(z)-\wp(\omega_1/2))(\wp(z)-\wp(\omega_2/2))(\wp(z)-\wp((\omega_1+\omega_2)/2))\\ &= C(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3),\end{aligned}$$

where C is some constant. It is easy to find C by comparing the coefficients of the lowest power of z in the Laurent expansion at the origin. Recall that $\wp(z)-z^{-2}$ is continuous at the origin, as is $\wp'(z)+2z^{-3}$. Thus, the leading term on the left is $(-2z^{-3})^2 = 4z^{-6}$, while on the right it is $C(z^{-2})^3 = Cz^{-6}$. We conclude that $C=4$. That is, $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = f(\wp(z)), \qquad \text{where} \quad f(x) = 4(x-e_1)(x-e_2)(x-e_3) \in \mathbb{C}[x]. \tag{6.1}$$

Notice that the cubic polynomial f has distinct roots (see Problem 4 of §5).

We now give another independent derivation of the differential equation for $\wp(z)$ which uses only Proposition 3 from §4. Suppose that we can find a cubic polynomial $f(x) = ax^3+bx^2+cx+d$ such that the Laurent expansion at 0 of the elliptic function $f(\wp(z))$ agrees with the Laurent expansion of $\wp'(z)^2$ through the negative powers of z. Then the difference $\wp'(z)^2 - f(\wp(z))$ would be an elliptic function with no pole at zero, or in fact anywhere else (since $\wp(z)$ and $\wp'(z)$ have a pole only at zero). By Proposition 3, this difference is a constant; and if we suitably choose d, the constant term in $f(x)$, we can make this constant zero.

To carry out this plan, we must expand $\wp(z)$ and $\wp'(z)^2$ near the origin. Since both are even functions, only even powers of z will appear.

Let c be the minimum absolute value of nonzero lattice points l. We shall take $r<1$, and assume that z is in the disc of radius rc about the origin. For each nonzero $l \in L$, we expand the term corresponding to l in the definition (4.1) of $\wp(z)$. We do this by differentiating the geometric series $1/(1-x) = 1+x+x^2+\cdots$ and then substituting z/l for x:

$$\frac{1}{(1-z/l)^2} = 1 + 2\frac{z}{l} + 3\frac{z^2}{l^2} + 4\frac{z^3}{l^3} + \cdots.$$

If we now subtract 1 from both sides, divide both sides by l^2, and then substitute in (4.1), we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l\in L\\ l\neq 0}} 2\frac{z}{l^3} + 3\frac{z^2}{l^4} + 4\frac{z^3}{l^5} + \cdots + (k-1)\frac{z^{k-2}}{l^k} + \cdots.$$

We claim that this double series is absolutely convergent for $|z| < rc$, in which case the following reversal of the order of summation will be justified:

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \cdots, \tag{6.2}$$

where for $k > 2$ we denote

$$G_k = G_k(L) = G_k(\omega_1, \omega_2) \underset{\text{def}}{=} \sum_{\substack{l \in L \\ l \neq 0}} l^{-k} = \sum_{\substack{m,n \in \mathbb{Z} \\ \text{not both } 0}} \frac{1}{(m\omega_1 + n\omega_2)^k} \tag{6.3}$$

(notice that the G_k are zero for odd k, since the term for l cancels the term for $-l$; as we expect, only even powers of z occur in the expansion (6.2)). To check the claim of absolute convergence of the double series, we write the sum of the absolute values of the terms in the inner sum in the form (recall: $|z| < r|l|$):

$$2|z| \cdot |l|^{-3} \cdot \left(1 + \frac{3}{2}r + \frac{4}{2}r^2 + \frac{5}{2}r^3 + \cdots\right) < \frac{2|z|}{(1-r)^2} \frac{1}{|l|^3},$$

and then use Lemma 2 from the proof of Proposition 6.

We now use (6.2) to compute the first few terms in the expansions of $\wp(z)$, $\wp(z)^2$, $\wp(z)^3$, $\wp'(z)$, and $\wp'(z)^2$, as follows:

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \cdots; \tag{6.4}$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4 \frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8)z^2 + \cdots; \tag{6.5}$$

$$\wp(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + \cdots; \tag{6.6}$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + \cdots. \tag{6.7}$$

Recall that we are interested in finding coefficients a, b, c, d of a cubic $f(x) = ax^3 + bx^2 + cx + d$ such that

$$\wp'(z)^2 = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d,$$

and we saw that it suffices to show that both sides agree in their expansion through the constant term. If we multiply equation (6.7) by a, equation (6.6) by b, equation (6.2) by c, and then add them all to the constant d, and finally equate the coefficients of z^{-6}, z^{-4}, z^{-2} and the constant term to the corresponding coefficients in (6.5), we obtain successively:

$$a = 4; \qquad b = 0; \qquad -24G_4 = 4(9G_4) + c; \qquad -80G_6 = 4(15G_6) + d.$$

Thus, $c = -60G_4$, $d = -140G_6$. It is traditional to denote

$$g_2 = g_2(L) \underset{\text{def}}{=} 60G_4 = 60 \sum_{\substack{l \in L \\ l \neq 0}} l^{-4};$$
$$g_3 = g_3(L) \underset{\text{def}}{=} 140G_6 = 140 \sum_{\substack{l \in L \\ l \neq 0}} l^{-6}. \tag{6.8}$$

We have thereby derived a second form for the differential equation (6.1):

$$\wp'(z)^2 = f(\wp(z)), \qquad \text{where} \quad f(x) = 4x^3 - g_2 x - g_3 \in \mathbb{C}[x]. \tag{6.9}$$

Notice that if we were to continue comparing coefficients of higher powers of z in the expansion of both sides of (6.9), we would obtain relations between the various G_k (see Problems 4–5 below).

The differential equation (6.9) has an elegant and basic geometric interpretation. Suppose that we take the function from the torus $\mathbb{C}/L$ (i.e., the fundamental parallelogram Π with opposite sides glued) to $\mathbb{P}^2_{\mathbb{C}}$ defined by

$$z \mapsto (\wp(z), \wp'(z), 1) \quad \text{for} \quad z \neq 0;$$
$$0 \mapsto (0, 1, 0). \tag{6.10}$$

The image of any nonzero point z of $\mathbb{C}/L$ is a point in the xy-plane (with complex coordinates) whose x- and y-coordinates satisfy the relationship $y^2 = f(x)$ because of (6.9). Here $f(x) \in \mathbb{C}[x]$ is a cubic polynomial with distinct roots. Thus, every point z in $\mathbb{C}/L$ maps to a point on the elliptic curve $y^2 = f(x)$ in $\mathbb{P}^2_{\mathbb{C}}$. It is not hard to see that this map is a one-to-one correspondence between $\mathbb{C}/L$ and the elliptic curve (including its point at infinity). Namely, every x-value except for the roots of $f(x)$ (and infinity) has precisely two z's such that $\wp(z) = x$ (see Problem 4 of §5). The y-coordinates $y = \wp'(z)$ coming from these two z's are the two square roots of $f(x) = f(\wp(z))$. If, however, x happens to be a root of $f(x)$, then there is only one z value such that $\wp(z) = x$, and the corresponding y-coordinate is $y = \wp'(z) = 0$, so that again we are getting the solutions to $y^2 = f(x)$ for our given x.

Moreover, the map from $\mathbb{C}/L$ to our elliptic curve in $\mathbb{P}^2_{\mathbb{C}}$ is analytic, meaning that near any point of $\mathbb{C}/L$ it can be given by a triple of analytic functions. Near non-lattice points of $\mathbb{C}$ the map is given by $z \mapsto (\wp(z), \wp'(z), 1)$; and near lattice points the map is given by $z \mapsto (\wp(z)/\wp'(z), 1, 1/\wp'(z))$, which is a triple of analytic functions near L.

We have proved the following proposition.

Proposition 10. *The map* (6.10) *is an analytic one-to-one correspondence between* $\mathbb{C}/L$ *and the elliptic curve* $y^2 = 4x^3 - g_2(L)x - g_3(L)$ *in* $\mathbb{P}^2_{\mathbb{C}}$.

One might be interested in how the inverse map from the elliptic curve to $\mathbb{C}/L$ can be constructed. This can be done by taking path integrals of $dx/y = (4x^3 - g_2 x - g_3)^{-1/2} dx$ from a fixed starting point to a variable endpoint. The resulting integral depends on the path, but only changes by

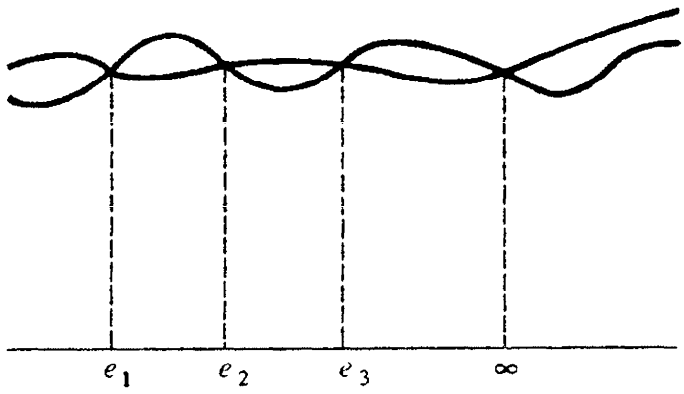

Figure I.10

a "period", i.e., a lattice element, if we change the path. We hence obtain a well-defined map to $\mathbb{C}/L$. See the exercises below for more details.

We conclude this section with a few words about an algebraic picture that is closely connected with the geometric setting of our elliptic curve. Recall from Proposition 8 that any elliptic function (meromorphic function on the torus $\mathbb{C}/L$) is a rational expression in $\wp(z)$ and $\wp'(z)$. Under our one-to-one correspondence in Proposition 10, such a function is carried over to a rational expression in x and y on the elliptic curve in the xy-plane (actually, in $\mathbb{P}^2_{\mathbb{C}}$). Thus, the field $\mathbb{C}(x, y)$ of rational functions on the xy-plane, when we restrict its elements to the elliptic curve $y^2 = f(x)$, and then "pull back" to the torus $\mathbb{C}/L$ by substituting $x = \wp(z)$, $y = \wp'(z)$, give us precisely the elliptic functions $\mathscr{E}_L$. Since the restriction of y^2 is the same as the restriction of $f(x)$, the field of functions obtained by restricting the rational functions in $\mathbb{C}(x, y)$ to the elliptic curve is the following quadratic extension of $\mathbb{C}(x)$: $\mathbb{C}(x)[y]/(y^2 - (4x^3 - g_2x - g_3))$. Algebraically speaking, we form the quotient ring of $\mathbb{C}(x)[y]$ by the principal ideal corresponding to the equation $y^2 = f(x)$.

Geometrically, projection onto the x-coordinate gives us Fig. I.10. Two points on the elliptic curve map to one point on the projective line, except at four points (the point at infinity and the three points where $y = 0$), where the two "branches" are "pinched" together.

In algebraic geometry, one lets the field $F = \mathbb{C}(x)$ correspond to the complex line $\mathbb{P}^1_{\mathbb{C}}$, and the field $K = \mathbb{C}(x, y)/y^2 - (4x^3 - g_2x - g_3)$ correspond to the elliptic curve in $\mathbb{P}^2_{\mathbb{C}}$. The rings $A = \mathbb{C}[x]$ and $B = \mathbb{C}[x, y]/y^2 - f(x)$ are the "rings of integers" in these fields. The maximal ideals in A are of the form $(x - a)A$; they are in one-to-one correspondence with $a \in \mathbb{C}$. A maximal ideal in B is of the form $(x - a)B + (y - b)B$ (where b is a square root of $f(a)$), and it corresponds to the point (a, b) on the elliptic curve.

$$\begin{array}{ccccc} K & \supset & B & \supset & (x-a)B + (y-b)B \qquad (b = \sqrt{f(a)}) \\ | & & | & & \\ | & & | & & (x-a)B + (y+b)B \\ | & & | & & | \\ F & \supset & A & \supset & (x-a)A \end{array}$$