Complex elliptic curves

David Blättler, Emil Staikov

13.03.2024

We have now established many fundamental properties of elliptic functions in general and the Weierstrass $\wp$-function in particular. We can now go further and use these properties to establish a bijection between the fundamental parallelogram of an arbitrary lattice $\Omega \subseteq \mathbb{C}$ and a particular elliptic curve. We will use this bijection to transfer the simple group law of the fundamental parallelogram over to the elliptic curve, which yields a very interesting geometric operation. Going back again, we will recover the so-called addition theorem for the $\wp$-function.

The $\wp$-function and elliptic curves

Recall from the previous talk the following differential equation for the $\wp$-function for a fixed lattice $\Omega \subseteq \mathbb{C}$.

Lemma 1. *For $z \in \mathbb{C} \setminus \Omega$, the $\wp$-function satisfies*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{1}$$

where $g_2 = g_2(\Omega) = 60G_4(\Omega)$ and $g_3 = g_3(\Omega) = 140G_6(\Omega)$ are the Weierstrass invariants of Ω.

Recall that for $k \in \mathbb{N}$, $k \geq 3$,

$$G_k(\Omega) = \sum_{0 \neq w \in \Omega} w^{-k}$$

is the absolutely convergent Eisenstein series for Ω.
Substituting $X = \wp(z)$ and $Y = \wp'(z)$ yields

$$Y^2 = 4X^3 - g_2X - g_3$$

which is the equation of an elliptic curve. This shows that for $z \in \mathbb{C}$, points of the form $(\wp(z), \wp'(z))$ lie on an elliptic curve. To make this correspondence exact, let

$$E(\Omega) = \{(X, Y) \in \mathbb{C}^2 : Y^2 = 4X^3 - g_2(\Omega)X - g_3(\Omega)\}$$
$$\overline{E}(\Omega) = E(\Omega) \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity, which we will simply think of as (∞, ∞). Consider now the map corresponding to the substitution made above:

$$\begin{aligned} \Phi : \mathbb{C}/\Omega &\longrightarrow \overline{E}(\Omega) \\ z + \Omega &\longmapsto (\wp(z), \wp'(z)) \end{aligned}$$

Note that we added the point at infinity so that the coset of 0, which is exactly Ω and where both $\wp$ and $\wp'$ have poles, also corresponds to a point on the elliptic curve. To investigate the properties of Φ, recall the following result from the last talk:

Lemma 2. *Suppose $\Omega = w_1\mathbb{Z} + w_2\mathbb{Z}$ and let $P = P(w_1, w_2)$ be a fundamental parallelogram. In addition, let $w_3 = w_1 + w_2$ and*

$$e_1 = \wp(w_1/2) \qquad e_2 = \wp(w_2/2) \qquad e_3 = \wp(w_3/2)$$

Then for $k \in \{1, 2, 3\}$, $\wp(z) - e_k$ has precisely one double root in P, namely at $w_k/2$, and for $x \in \mathbb{C} \setminus \{e_1, e_2, e_3\}$ fixed, $\wp(z) - x$ has precisely two simple roots in P.

We can now show the following

Proposition 1. *The map $\Phi : \mathbb{C}/\Omega \longrightarrow \overline{E}(\Omega)$ is well-defined and a bijection.*

Proof. The definition of Φ is invariant under choice of representative because $\wp$ and $\wp'$ are elliptic. The differential equation (1) shows that the image of Φ is contained in $\overline{E}(\Omega)$. Thus, Φ is well-defined.

To show that Φ is surjective, let $(X, Y) \in \overline{E}(\Omega) \setminus \{\mathcal{O}\}$. By Lemma 2, there is some $z \in \mathbb{C}$ such that $\wp(z) = X$. By equation (1), we have

$$Y^2 = 4X^3 - g_2X - g_3 = 4\wp(z)^3 - g_2\wp(z) - g_3 = \wp'(z)^2$$

so either $\wp'(z) = Y$ or $\wp'(z) = -Y$. Since $\wp$ is even and $\wp'$ is odd, we may replace z by $-z$ to get $(\wp(z), \wp'(z)) = (X, Y)$. Since Ω maps to $\mathcal{O}$, Φ is surjective.

To show that Φ is injective, suppose that there are $z_1, z_2 \in \mathbb{C} \setminus \Omega$ such that $\Phi(z_1 + \Omega) = \Phi(z_2 + \Omega)$. We first consider only the equality $\wp(z_1) = \wp(z_2)$.
If $\wp(z_1) \in \{e_1, e_2, e_3\}$, then by Lemma 2, $z_1 \equiv z_2 \pmod{\Omega}$, as $\wp$ assumes each of these values only once in a given fundamental parallelogram. Otherwise, again by Lemma 2, the value $\wp(z_1)$ is assumed at exactly two distinct points in a fundamental parallelogram. Since $\wp$ is even and $\wp(z_1) \notin \{e_1, e_2, e_3\}$, so $z_1 \notin \{w_1/2, w_2/2, w_3/2\}$, these two distinct points are z_1 and $-z_1 \pmod{\Omega}$. Thus, $z_1 \equiv \pm z_2 \pmod{\Omega}$.
We now consider the equality $\wp'(z_1) = \wp'(z_2)$. If $\wp'(z_1) \neq 0$, then since $\wp'$ is odd, $\wp'(z_1) \neq \wp'(-z_1)$ and so we have $z_1 \equiv z_2 \pmod{\Omega}$. If $\wp'(z_1) = 0$, then by Lemma 2, we have $z_1 \equiv w_k/2 \pmod{\Omega}$ for some $k \in \{1, 2, 3\}$ and so $z_1 \equiv -z_1 \pmod{\Omega}$. Thus in all cases, $z_1 \equiv z_2 \pmod{\Omega}$.
Lastly, $\wp$ has poles exactly on Ω, so only Ω maps to $\mathcal{O}$. Thus, Φ is injective. $\square$

Note that g_2 and g_3 uniquely determine Ω and the coefficients of an elliptic curve uniquely determine the curve, so this correspondence assigns a unique elliptic curve to each lattice. In addition, given g_2 and g_3 with $g_2^3 - 27g_3^2$, we can find a lattice Ω with such Weierstrass invariants. Thus, $\overline{E}(\Omega)$ is an elliptic curve of nearly general form.
Since Φ is a continuous, bijective function defined on a compact set, it is a homeomorphism. This shows that elliptic curves of the form $\overline{E}(\Omega)$ are topologically equivalent to the torus $\mathbb{C}/\Omega$.

A group structure on elliptic curves

If we define addition on $\mathbb{C}/\Omega$ as $(u+\Omega)+(v+\Omega) := (u+v)+\Omega$, then we can carry over the natural group structure of $\mathbb{C}/\Omega$ to the elliptic curve $\overline{E}(\Omega)$ using the bijection Φ.

Definition 1. We define addition on the elliptic curve $\overline{E}(\Omega)$ as

$$P + Q := \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)). \tag{2}$$

for $P, Q \in \overline{E}(\Omega)$ arbitrary.

Proposition 2. *The elliptic curve $\overline{E}(\Omega)$ with the addition 2 is an abelian group with unit element $\mathcal{O}$ and Φ is a group isomorphism between $\mathbf{C}/\Omega$ and $\overline{E}(\Omega)$. Moreover for $z \in \mathbb{C}/\Omega$, the inverse can be computed as*

$$-(\wp(z), \wp'(z)) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) \tag{3}$$

Furthermore for $u, v \in \mathbb{C}$ with $u, v, u+v \notin \Omega$, we have

$$(\wp(u), \wp'(u)) + (\wp(v), \wp'(v)) = (\wp(u+v), \wp'(u+v)) \tag{4}$$

Remark. Equation (3) tells us that the inverse of a point $(X, Y) = P \in \overline{E}(\Omega)$ is calculated as

$$-P = (X, -Y).$$

Proposition 2 does not give us a direct way to calculate $P + Q$ just from the components of P and Q. This will be the goal of the next part of this script. We will first introduce a different, geometric way of adding points on the elliptic curve $\overline{E}(\Omega)$, which we will then use to express $P + Q$.

The geometric addition law

Instead of directly stating the formulas for the geometric addition, we will instead motivate the ideas required to derive them and see why the different case distinctions are necessary and also sensible.

Motivation of the definition

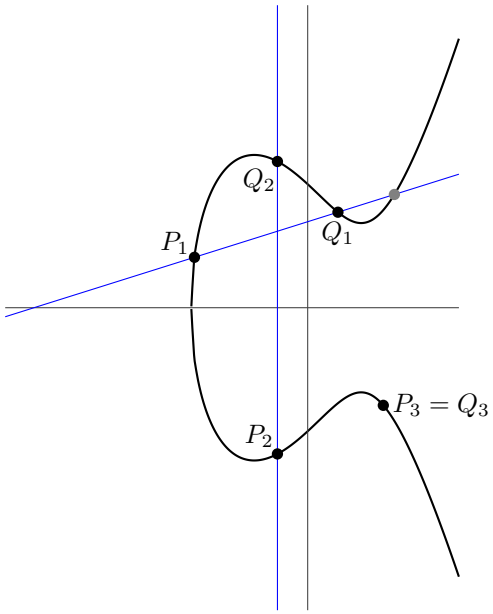
Having seen the addition law defined on $\overline{E}(\Omega)$ as above, we will now find a way of defining the sum of two points in $\overline{E}(\Omega)$ geometrically on said elliptic curve. This is **not** the same addition as before, but as we will see, it is very closely connected to it. To distinguish the two laws, we will denote the geometric sum of P and Q as $P \bullet Q$.

We still want $\mathcal{O} = (\infty, \infty)$ to be our neutral element. Thus we have that $\forall P \in \overline{E}(\Omega)$:

$$P \bullet \mathcal{O} = \mathcal{O} \bullet P = P$$

Now we are left with defining $P \bullet Q$ for $P, Q \in E$. The main idea behind our geometric addition is, to connect the points P, Q by a complex line and observe where it hits the elliptic curve a third time.

In order to display this, we will set g_2, g_3 to be real and only observe the real image of E.



In the usual case, as seen in with the points $P_1, Q_1 \in E$, the line does indeed intersect the elliptic curve a third time. But we can also find exceptions, where this doesn't seem to be the case.
For instance, the line connecting points $P_2, Q_2 \in E$, which lie above one another, does not intersect any other point in E.
Also, if our points are the same, as in the case of $P_3, Q_3 \in E$, we do not even know in which direction the complex line connecting the two, should face.

Case distinctions

This motivates us to split up our calculations into three distinct cases. In order to more closely examine these cases, we will introduce the notation that $P = (X_P, Y_P)$ for points $P \in \mathbb{C}^2$.

Case 1: $X_P \neq X_Q$

If the two points do not lie above each other, we can write the line connecting the two as a equation $Y = a_{P,Q}X + b_{P,Q}$, where $a_{P,Q}$ is the slope of the line and $b_{P,Q}$ the offset. We can calculate them as follows:

$$\begin{aligned} a_{P,Q} &:= \frac{Y_P - Y_Q}{X_P - X_Q} \\ b_{P,Q} := Y_P - a_{P,Q}X_P &= \frac{X_P Y_Q - X_Q Y_P}{X_P - X_Q} \end{aligned} \tag{5}$$

This line will always intersect the line a third time, the reason for which will be given after having been introduced to the other two cases.
For now, we will claim that there is indeed a third intersection point $P \bullet Q \in E$, which we can calculate as having the coordinates

$$\begin{aligned} X_{P\bullet Q} &:= \frac{1}{4}a_{P,Q}^2 - X_P - X_Q, \\ Y_{P\bullet Q} &:= a_{P,Q}X_{P\bullet Q} + b_{P,Q}. \end{aligned} \tag{6}$$

The definition of $Y_{P,Q}$ directly shows that the point $P \bullet Q$ does indeed lie on the line connecting P and Q.
In order to show that it also lies on the elliptic curve, we will use the following lemma.

Lemma 3. *For $X \in \mathbb{C}$ we have*

$$4X^3 - g_2X - g_3 = 4(X - X_P)(X - X_Q)(X - X_{P\bullet Q}) + (a_{P,Q}X + b_{P,Q})^2,$$

Proof. We will rewrite the equation as

$$\begin{aligned} 4X^3 - g_2X - g_3 = 4X^3 &+ X^2(-4X_P - 4X_Q - 4X_{P\bullet Q} + a_{P,Q}^2) \\ &+ X(4X_PX_Q + 4X_PX_{P\bullet Q} + 4X_QX_{P\bullet Q} + 2a_{P,Q}b_{P,Q}) \\ &+ (-4X_PX_QX_{P\bullet Q} + b_{P,Q}^2) \end{aligned}$$

We clearly see that the coefficients of X^3 cancel out on both sides. Also, if we insert our definition of $X_{P\bullet Q}$ from 6, we get that the coefficient for the X^2 term on the right hand ends up simplifying to

$$\begin{aligned} &- 4X_P - 4X_Q - 4X_{P\bullet Q} + a_{P,Q}^2 \\ =&- 4X_P - 4X_Q - 4\left(\frac{1}{4}a_{P,Q}^2 - X_P - X_Q\right) + a_{P,Q}^2 = 0 \end{aligned}$$

which coincides with the according coefficient on the left side.
We see that the difference between the left and right side is linear in X. But as the difference is clearly 0 for the two distinct points X_P, X_Q and also since P, Q lie on the intersection between the line and E, the difference must vanish everywhere, resulting in the equation being correct. □

Now using the proven equation, we can show that $P \bullet Q$ does indeed lie on the elliptic curve. If we let X to be equal to $X_{P \bullet Q}$ we get the equation

$$4X_{P\bullet Q}^3 - g_2 X_{P\bullet Q} - g_3 = (a_{P,Q} X_{P\bullet Q} + b_{P,Q})^2 = Y_{P\bullet Q}^2,$$

which we have seen, characterizes the points on the elliptic curve.

Case 2: $P \neq Q$**,** $X_P = X_Q$

This is the case which had been illustrated by the points P_2, Q_2 in the illustration above. Using the defining equation for the elliptic curve, we get that

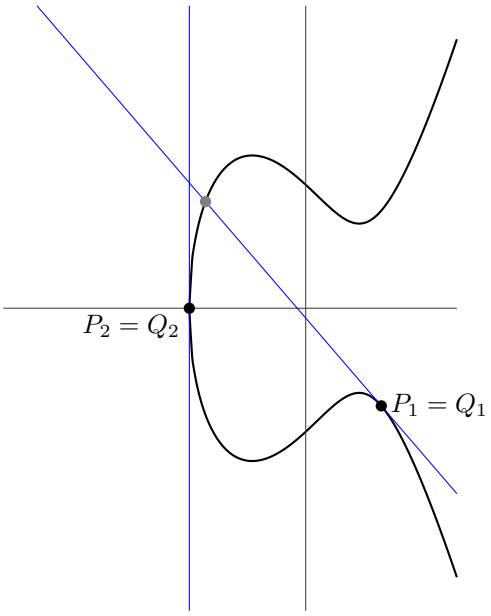
$$Y_P^2 = 4X_P^3 - g_2 X_P - g_3 = 4X_Q^3 - g_2 X_Q - g_3 = Y_Q^2,$$

which implies that $Y_P = \pm Y_Q$. In particular, as $P \neq Q$, we get that $Y_P = -Y_Q$. We notice that the line connecting P and Q is vertical and that we cannot use the same approach as in case 1, as the slope of tis line would be ∞.

Furthermore, even if we could, there is no third intersection point, which we could calculate. But since we have defined $\mathcal{O}$ as being the point (∞, ∞), we define $P \bullet Q$ to be equal to $\mathcal{O}$, which we can justify as the vertical line "intersecting" the elliptic curve at infinity.

Case 3: $P = Q$

If our two points are indeed the same, we cannot use either the methods of the first or second case, as we do not know in which direction the complex line connecting the two, should point. As will be made apparent shortly, it is sensible, to regard the line, which is tangent to the elliptic curve for this case.



We can see that in almost all cases this results in another intersection with the elliptic curve. The only time this is not the case is, when we have that $Y_P = Y_Q = 0$, in which case the tangent line will be vertical. Similar to case 2, we will define $P \bullet Q = \mathcal{O}$ in this case.

In the usual case where $Y_P = Y_Q \neq 0$, we can describe the tangent line with the equation $Y = a_P X + b_P$, where a_P is the slope of the line. If we differentiate the equation characterizing the elliptic curve with respect to X on both sides we get

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}X} Y^2 &= \frac{\mathrm{d}}{\mathrm{d}X} \left(4X^3 - g_2 X - g_3\right) \\ \Rightarrow 2YY' &= 12X^2 - g_2 \\ \Rightarrow Y' &= \frac{12X^2 - g_2}{2Y} \end{aligned}$$

This leads us to the formulas for a_P, b_P:

$$\begin{aligned} a_P &:= \frac{12X_P^2 - g_2}{2Y_P}, \\ b_P &:= Y_P - a_P X_P \end{aligned} \tag{7}$$

The same way as in case 2, we can now define the point $P \bullet P$ through its coordinates as

$$\begin{aligned} X_{P \bullet P} &:= \frac{1}{4} a_P^2 - 2X_P, \\ Y_{P \bullet P} &:= a_P X_{P \bullet P} + b_P. \end{aligned} \tag{8}$$

The same way as in the second case, we can prove that this is indeed the intersection point of the tangent line and the elliptic curve.

Using Bézout's theorem

The way we've introduced geometric addition required a lot of tedious case distinctions, which it would be nice to avoid. In fact, there exists an alternative approach which allows us to treat all cases uniformly.
We once again start with the idea of connecting the two points by a complex line and then intersecting it with $\overline{E}(\Omega)$. Before, this lead to problems in cases 2 and 3. Using *Bézout's theorem*, we can see that in reality, this is no problem. *Bézout's theorem* is a statement in algebraic geometry concerning the number of solutions of polynomials. In particular for our case, because the line is defined by a degree 1 polynomial and the elliptic curve is defined by a degree 3 polynomial, *Bézout's theorem* tells us that we will expect to have $1 \cdot 3 = 3$ roots counting multiplicity.

Using this, our original idea can explain the entire idea behind geometric addition without the need of the many case distinctions. For instance, in case 3, we see that in reality there are 3 roots when the tangent point is counted twice, as it has a multiplicity of 2. Also, looking at case 2 through the lens of projective geometry, we can define $\mathcal{O}$ to really be the third intersection point of the complex line and the elliptic curve. While the theorem gives the existence of the

third intersection point and thus instantly shows that the geometric addition is well-defined, it is a non-constructive result, and the relation between $P \bullet Q$ and $P + Q$ becomes less evident.

The complete definition of $P \bullet Q$

We have seen the formulas for $P \bullet Q$ for the different cases. We will now combine these in order to get the entire formula for $P \bullet Q$.

Definition 2. The geometric addition on $\overline{E}(\Omega)$ is defined as

$$P \bullet Q := \begin{cases} P & \text{if } Q = \mathcal{O} \\ Q & \text{if } P = \mathcal{O} \\ \text{formula 6} & \text{if } P \neq Q \in E(\Omega) \text{ and } X_P \neq X_Q \\ \mathcal{O} & \text{if } P \neq Q \in E(\Omega) \text{ and } X_P = X_Q \\ \text{formula 8} & \text{if } P = Q \in E(\Omega) \text{ and } Y_P \neq 0 \\ \mathcal{O} & \text{if } P = Q \in E(\Omega) \text{ and } Y_P = 0 \end{cases} \tag{9}$$

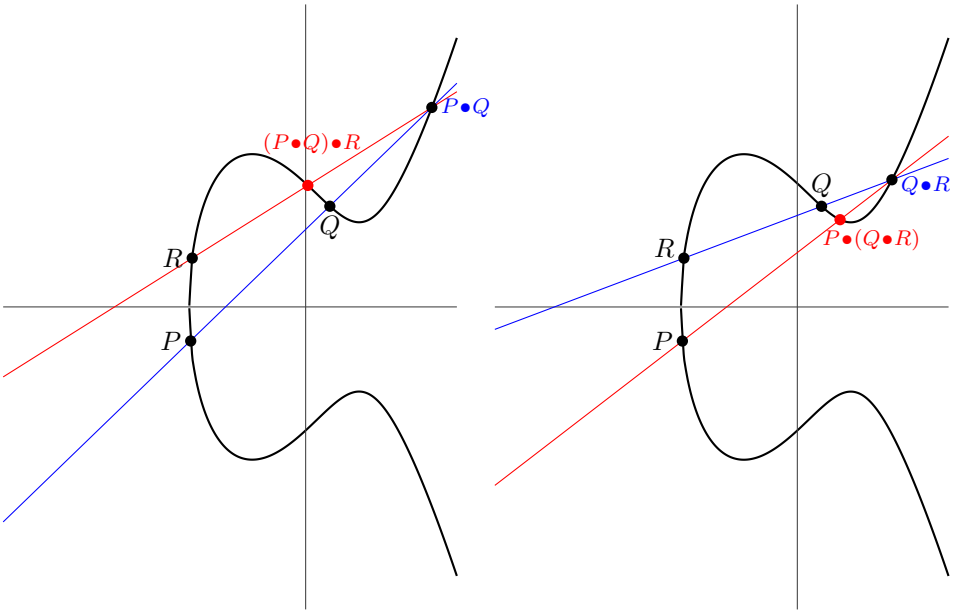
Comparing $P \bullet Q$ to $P + Q$

We have seen the definitions for both kinds of additions of point in $\overline{E}(\Omega)$. As mentioned earlier, these are not the same, but are closely connected. In this section we will figure out what this aforementioned connection is. First, it is sensible to take a look at the properties of $P \bullet Q$.

Remark. The geometric addition law $P \bullet Q$ does not give a group structure on $\overline{E}(\Omega)$ as it is not associative.

This can be observed in the following two figures, where we see that

$$(P \bullet Q) \bullet R \neq P \bullet (Q \bullet R).$$



Theorem 1. *For $u, v, w \in \mathbb{C} \setminus \Omega$ such that $u + v + w \in \Omega$ and $w + \Omega \notin \{u + \Omega, v + \Omega\}$, then we have that*

$$\Phi(u) \bullet \Phi(v) = \Phi(w).$$

Proof. To simplify the proof, let us define the points

$$P = \Phi(u), \quad Q = \Phi(v), \quad R = \Phi(w).$$

We first look at the case when $u + \Omega \neq v + \Omega$, meaning $P \neq Q$. This implies that $X_P \neq X_Q$. Indeed, if it were, then $X_P = \wp(u) = \wp(v) = X_Q$ would give us that $u + v \in \Omega$ due to the fact that $\sum_{p \in P}(\text{ord}_c(f)) \cdot c \in \Omega$ for any fundamental parallelogram P. This in turn implies that either $u + v + w \in \Omega$ or $w \notin \Omega$ is false.
This means that for calculating $P \bullet Q$, we are in case 1. In particular in order to show that $P \bullet Q = R$, we must check that R is the third intersection point of E and the complex line connecting P, Q. In order to do this, we define the function

$$f(z) := \wp'(z) - (a_{P,Q}\wp(z) + b_{P,Q}).$$

This function is derived from the formula $Y = a_{P,Q}X + b_{P,Q}$, where we replace (X, Y) by $(\wp, \wp')$ in such a way that the roots of the function are exactly the points which lie on the complex line connecting P, Q. The function f has a pole of order 3 at the point $z = 0$ and no other poles in $\mathbb{C}/\Omega$, so it will have three roots in $\mathbb{C}/\Omega$.
Since these roots coincide with the points on the line, we know that P and Q are roots, meaning that $f(P) = f(Q) = 0$. Thus since $f(w)$ has three roots in $\mathbb{C}/\Omega$ whose sum lies in Ω, this means that $f(w) = 0$. This shows that the point $R = \Phi(w)$ is indeed the third intersection point of E with the line connecting P, Q, meaning we have $P \bullet Q = R$.
Now we simply need to check that this is also the case if $u + \Omega = v + \Omega$, that is $P = Q$. In this case we have that $u + v + w = 2u + w \in \Omega$. The fact that $u, w \notin \Omega$ gives us that $2u \notin \Omega$ meaning that $\wp'(u) \neq 0$. Thus we are in case 3 for the geometric addition law, in particular since $Y_P \neq 0$, we will can get $P \bullet Q$ as the intersection of E and the tangent line through P. Similar to above, we consider the function

$$f(z) := \wp'(z) - (a_P\wp(z) + b_P).$$

We see that the roots of f are the points on the tangent line through P. It has an order three pole at $z = 0$ and three roots in $\mathbb{C}/\Omega$. Thus we have $f(u) = 0$ and if we take the derivative of the differential equation $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ we get

$$\begin{aligned} 2\wp''(z) \cdot \wp'(z) &= 12\wp(z)^2 \cdot \wp'(z) - g_2 \cdot \wp'(z) \\ \Rightarrow \wp''(z) &= \frac{12\wp(z)^2 - g_2}{2} \end{aligned}$$

Meaning that if we use this and the definition for a_P, we get that

$$\begin{aligned} f'(u) &= \wp''(u) - a_P\wp'(u) \\ &= \frac{12\wp(u)^2 - g_2}{2} - \frac{12\wp(u)^2 - g_2}{2\wp'(u)}\wp'(u) = 0 \end{aligned}$$

which leads us to conclude that $z = u$ is a double root of f. The third root must then be $w \bmod \Omega$ in order for their sum to be in Ω. Thus we get that $\Phi(w)$ is indeed the intersection point between E and the tangent line through the point P. We get that $P \bullet P = R$, so the claimed formula also holds in this second case. □

Definition 3. For a point $P = (X_P, Y_P) \in \mathbb{C}^2$, we define

$$P^* := (X_P, -Y_P).$$

With Theorem 1, we can now see the similarity between the two addition laws and show that they essentially agree with each other. In particular, we get the following proposition:

Proposition 3. *The addition law $E(\Omega) \times E(\Omega) \to E(\Omega)$ given by $(P, Q) \mapsto P + Q$, satisfies*

$$P + Q = (P \bullet Q)^* \qquad \text{if } P \neq Q$$

and

$$P + P = (P \bullet P)^* \qquad \text{if } Y_P \neq 0$$

Proof. Let $P = \Phi(u)$ and $Q = \Phi(v)$, then define the point $w = -u - v$. We can then use Theorem 1 to get that

$$\begin{aligned} P + Q &= \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)) = \Phi(u + v) = \Phi(-w) \\ &= (\wp(-w), \wp'(-w)) = (\wp(w), -\wp'(w)) = (\Phi(w))^* \\ &= (P \bullet Q)^* \end{aligned}$$

which closes the proof. □

In particular, we can now use the formula for the geometric addition law 9, to get formulas for the coordinates of the sum $P + Q$:

$$X_{P+Q} = \frac{1}{4}a_{P,Q}^2 - X_P - X_Q, \qquad Y_{P+Q} = -a_{P,Q}X_{P+Q} - b_{P,Q} \qquad \text{if } X_P \neq X_Q$$

and

$$X_{2P} = \frac{1}{4}a_P^2 - 2X_P \qquad Y_{2P} = -a_P X_{2P} - b_P \qquad \text{if } Y_P \neq 0$$

which also gives us that $-P = P^* = (X_P, -Y_P)$.

Remark. If we set $\mathcal{O}^* = \mathcal{O}$, then Proposition 3 gives us that actually

$$P + Q = (P \bullet Q)^*$$

for all $P, Q \in \overline{E}(\Omega)$. We can check the remaining cases to be true. If $P \neq Q$ with $X_P = X_Q$, we get that $P + Q = \mathcal{O} = (P + Q)^*$. And if $P = Q$ with $Y_P = 0$, we respectively see that $2P = \mathcal{O} = (P \bullet P)^*$.

The addition theorem for $\wp$

Using the geometric properties of the group operation on elliptic curves we just proved, we can extract the so-called addition theorem for the Weierstrass $\wp$-function using the bijection Φ. To this end, let $u, v, w \in \mathbb{C} \setminus \Omega$ be such that $u + v + w = 0$ and $u + \Omega$, $v + \Omega$ and $w + \Omega$ are pairwise different. By Theorem 1, we then have

$$\Phi(u) \bullet \Phi(v) = \Phi(w) \tag{10}$$

Setting $P = \Phi(u)$, $Q = \Phi(v)$ and $R = \Phi(w)$ and considering only the first coordinate in equation (10), we get that

$$\begin{aligned}\wp(w) = X_R &= \frac{1}{4}a_{P,Q}^2 - X_P - X_Q = \frac{1}{4}\left(\frac{Y_P - Y_Q}{X_P - X_Q}\right)^2 - X_P - X_Q \\ &= \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v)\end{aligned}$$

Since $\wp$ is even and $u + v + w = 0$, we have $\wp(u + v) = \wp(-w) = \wp(w)$, so

$$\wp(u + v) = \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v)$$

By considering this equation as an abstract equality of elliptic functions, we can remove some of the restrictions imposed on u and v and get a more general

Theorem 2 (Addition theorem)**.** *For $z, w \in \mathbb{C}$ with $z, w, z \pm w \notin \Omega$, we have*

$$\wp(z + w) = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2 - \wp(z) - \wp(w) \tag{11}$$

To show this theorem, we first show some properties of the function on the right side in the following

Proposition 4. *For a fixed $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$, the function*

$$f_w(z) = \frac{1}{2}\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}$$

is an elliptic function with respect to Ω with poles of first order exactly at the points $z \in \Omega$ and $z \in -w + \Omega$ and Laurent expansions

$$\begin{aligned}f_w(z) &= -\frac{1}{z} - \wp(w)z + O(z^2) \\ f_w(z) &= \frac{1}{z + w} + c(w) + O(z + w)\end{aligned}$$

around $z = 0$ and $z = -w$ respectively, where $c(w) \in \mathbb{C}$ is a constant.

Proof. f_w is elliptic as the composition of elliptic functions. $f_w(z)$ is not defined for $z \in \Omega$, $z \in w + \Omega$ and $z \in -w + \Omega$, but

$$\lim_{z \to w} f_w(z) = \frac{1}{2}\lim_{z \to w}\frac{(\wp'(z) - \wp'(w))/(z - w)}{(\wp(z) - \wp(w))/(z - w)} = \frac{\wp''(w)}{2\wp'(w)}$$

since $w \notin \frac{1}{2}\Omega$, so $\wp'(w) \neq 0$. Thus, the singularities in $w + \Omega$ are removable.
To determine the Laurent expansion of f_w around 0, recall that around $z = 0$, we have $\wp(z) = z^{-2} + O(z^2)$ and $\wp'(z) = -2z^{-3} + O(z)$. Some manipulation of these series yields the desired Laurent expansion.
For the Laurent expansion around $z = -w$, note that since $w \notin \frac{1}{2}\Omega$, Lemma 2 shows that $\wp(z) - \wp(w)$ has a simple root at every $z \in -w + \Omega$ and since $\wp'$ is odd, $\wp'(z) - \wp'(w) = -2\wp'(w) \neq 0$, again by Lemma 2. Thus, f_w has a simple pole at every $z \in -w+\Omega$ and since the residue at $z \in \Omega$ is -1, Liouville's second theorem shows that the residue at w must be 1. Thus, around $z = -w$,

$$f_w(z) = \frac{1}{z+w} + c(w) + O(z+w)$$

which closes the proof of the Proposition. □

We can now go on to prove Theorem 2

Proof. For a fixed $w \in \mathbb{C} \setminus \frac{1}{2}\Omega$, we consider

$$g(z) = f_w(z)^2 - \wp(z+w) - \wp(z) - \wp(w)$$

g is elliptic as the composition of elliptic functions and holomorphic apart from possible poles at $z \in \Omega$ and $z \in -w + \Omega$, as f_w and $\wp$ have poles there and nowhere else. With the Laurent expansions derived in Proposition 4, we get that at $z = 0$

$$\begin{aligned} g(z) &= (-z^{-1} - \wp(w)z + O(z^2))^2 - (\wp(w) + O(z)) - (z^{-2} + O(z^2)) - \wp(w) \\ &= z^{-2} + 2\wp(w) - \wp(w) - z^{-2} - \wp(w) + O(z) = O(z) \end{aligned}$$

and at $z = -w$

$$\begin{aligned} g(z) &= ((z+w)^{-1} + c(w) + O(z+w))^2 - ((z+w)^{-2} + O(z+w)) + O(1) \\ &= (z+w)^{-2} + 2c(w)(z+w)^{-1} - (z+w)^{-2} + O(1) \\ &= 2c(w)(z+w)^{-1} + O(1) \end{aligned}$$

If we had $c(w) \neq 0$, g would have simple poles at all $z \in -w + \Omega$ and no other poles. This however contradicts Liouville's second theorem, which states that the sum of all residues of an elliptic function in any fundamental domain must be 0. Thus, $c(w) = 0$ and g is holomorphic everywhere. By Liouville's first theorem, g is constant. Since $g(z) = O(z)$ around zero, we have $g(0) = 0$, so g is identically zero.
For $w \in \frac{1}{2}\Omega \setminus \Omega$, the addition theorem follows by continuity, since both sides of equation (11) are holomorphic near such w. □

By taking the limit as $w \to z$ and using the differential equation (1), we can recover the following

Corollary 1 (Duplication formula)**.** *For $z \in \mathbb{C} \setminus \frac{1}{2}\Omega$, we have*

$$\wp(2z) = \frac{1}{4}\left(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\right)^2 - 2\wp(z) \tag{12}$$

Proof. We first consider the limit of equation (11) as $w \to z$. With l'Hospital's rule, we get

$$\lim_{w\to z} \frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} = \lim_{w\to z} \frac{\wp''(w)}{\wp'(w)} = \frac{\wp''(z)}{\wp'(z)}$$

where the second limit exists because $\wp''$ has poles only in Ω and $\wp'$ has zeroes only in $\frac{1}{2}\Omega$, and z is contained in neither.
Thus, equation (11) in the limiting case yields

$$\wp(2z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z) \tag{13}$$

Taking the derivative of differential equation (1) yields

$$2\wp''(z) = 12\wp(z)^2 - g_2$$

since $z \notin \Omega$. Substituting this in equation (13) gives the desired result. □

Note that the duplication formula also arises from Theorem 1 by taking $u = v$.

References

[1] M. Schwagenscheidt, *Elliptic functions*, lecture notes, available online.

[2] E. Freitag, R. Busam, *Funktionentheorie*, Springer (1993).