1 Notes on Weierstrass Uniformization

1.1 Overview

The goal of these notes is to explain Weierstrass Uniformization. Here's the outline.

- §1.2: We define a *lattice* $\Lambda \subset C$. Informally, Λ is an infinite grid containing 0. The quotient C/Λ turns out to be a torus and a group.
- §1.3: We construct a function P : C → C ∪ ∞ called the Weierstrass P function. This function turns out to be Λ-periodic, in the sense that P(z + λ) = P(z) for all z. This means that P induces a well defined map from C/Λ into C ∪ ∞.
- §1.4: We define what a *holomorphic* function is, show that the Weierstrass P function is holomorphic, and we compute the complex derivative P' of P.
- $\S1.5$: We show that *P* satisfies the differential equation

$$(P')^2 = 4P^3 + g_2P + g_3. \tag{1}$$

The constants g_2 and g_3 depend on the lattice Λ .

• We now define

$$\Psi(z) = (P(z), P'(z)). \tag{2}$$

The image of Ψ is an elliptic curve which, under a very simple change of coordinates, becomes a Weierstrass elliptic curve! For completeness, we define $\Psi(z) = [0:1:0]$ when $z \in \Lambda$.

• The remaining sections deal with the fine points of the equation above. In particular, we apply tools from complex analysis to show that Ψ is a bi-holomorphism and a group isomorphism. "bi-holomorphism" means a bijective complex analytic map whose inverse is also complex analytic. It is the isomorphism in the category of Riemann surfaces.

1.2 Lattices

A *lattice* in C is a set of points of the form

$$\Lambda = \{ m\alpha + n\beta \quad m, n \in \mathbf{Z} \}, \tag{3}$$

where α and β are not real multiples of each other. The set of points in Λ forms a grid of parallelograms. The classic case is when $\alpha = 1$ and $\beta = i$. In this case $\Lambda = \mathbf{Z}[i]$, the Gaussian integers.

The quotient C/Λ has several nice properties.

- 1. C/Λ is homeomorphic to a torus namely, a single parallelogram with its sides identified.
- 2. C/Λ abelian group under addition, since both C and Λ are abelian groups under addition.

A map $f : \Lambda \to \mathbb{C} \cup \infty$ is called Λ -periodic if $f(\lambda + z) = f(z)$ for all $z \in \mathbb{C}$ and all $\lambda \in \Lambda$. In this case, f induces a map from \mathbb{C}/Λ into $\mathbb{C} \cup \infty$. This new map is usually also denoted by f.

1.3 The Weierstrass Function

Let Λ be any lattice. Informally, the function we are interested in is

$$\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^2} \tag{4}$$

The nice thing about this "function" is that it is clearly Λ -periodic. The bad thing is that the series above does not converge, so the "function" does not exist.

The Weierstrass function is the function that the expression in Equation 4 wants to be. Here is the definition.

$$P(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \frac{2z\lambda - z^2}{\lambda^2 (z-\lambda^2)}.$$
 (5)

To study the convergence of this series, choose $z \notin \Lambda$. For all λ sufficiently large, we have the estimate

$$\left|\frac{z^2 - 2z\lambda}{\lambda^2(z - \lambda^2)}\right| < \frac{C_z}{|\lambda|^3}.$$
(6)

Here C_z is a constant that depends on z in a way that we don't care about. The series in Equation 5 does converge because the corresponding series

$$\sum_{\lambda \neq 0} \frac{1}{|\lambda|^3}$$

converges.

The Weierstrass function P(z) is defined for all $z \in \mathbb{C} - \Lambda$. As $z \to \lambda \in \Lambda$, the quantity |P(z)| tends to ∞ . We define $P(\lambda) = \infty$ for $\lambda \in \Lambda$.

Periodicity and Evenness: We can describe Equation 5 in a way which makes it more clear that P is Λ -periodic. We choose some large disk Δ about the origin and we take the sum in Equation 4 over all points in $\Lambda \cap \Delta$. This gives us an enormous number. We then subtract off the sum of $1/\lambda^2$ for all nonzero $\lambda \in \Lambda \cap \Delta$. We then take the limit as the radius of Δ tends to ∞ . From this definition it is more clear that P is Λ -invariant.

This description also shows that P is an even function: P(-z) = P(z). The point is that the finite Δ -sum we just mentioned is an even function, by symmetry, and therefore so is the limit of these functions.

1.4 Holomorphic Functions

Let $U \subset C$ be an open set. Let us call a function $f : U \to C$ holomorphic point $z_0 \in U$ we have an equation

$$f(z) = \sum_{i=0}^{\infty} a_i (z - z_0)^i,$$
(7)

which holds as long as $|z - z_0|$ is smaller than the (nonzero) radius of convergence of the series. Here $a_i \in \mathbf{C}$. Convergent power series themselves are holomorphic within their open disk of convergence, so in practice if you can establish Equation 7 for some point z_0 , then a similar equation holds for all z_1 sufficiently close to z_0 .

Lemma 1.1 $P(z) - 1/z^2 = a_2 z^2 + a_4 z^4 + ...$ in some disk centered at 0.

Proof: $P(z) - 1/z^2$ is the sum of terms of the form

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}.$$

The series expansion for this term is

$$\frac{2z}{\lambda^3} + \frac{3z^2}{\lambda^4} + \frac{4z^3}{\lambda^5}.$$

Summing these over all λ it is not too hard to see everything converges to a single series of the form given in Equation 7. This gives the series $a_0 = 0$. All the odd terms in the series vanish because $P(z) - 1/z^2$ is an even function.

Lemma 1.2 P(z) is holomorphic in $C - \Lambda$.

Proof: Let $z_0 \in \mathbf{C} - \Lambda$ and let $H(z) = P(z_0 + z)$. It suffices to show that H equals a convergent power series at 0. The first term in H(z) is $1/(z_0 + z)^2$. As in the preceding result, this equals a power series in a neighborhood of 0. The remaining terms have the form

$$\frac{1}{(z-\lambda_*)^2} - \frac{1}{\lambda_*^2} + \left(\frac{1}{\lambda^2} - \frac{1}{\lambda_*^2}\right), \qquad \lambda_* = \lambda - z_0$$

If we ignore the terms in parentheses and sum, we get the same kind of series as above, with respect to the shifted grid $\bigcup_{\lambda \in \Lambda} \lambda - z_0$. Moreover, the sum of the terms in parentheses is finite. So, adding it all together, we get one convergent power series.

The *complex derivative* of a holomorphic function given f is given by the difference quotient

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}.$$
 (8)

This differs from the usual notion of a derivative because h is allowed to be complex. Here is a nice and relevant example. When $z \neq 0$ and $\phi(z) = 1/z^2$, we have $\phi'(z) = -2/z^3$. All the usual formulas for the differentiation of rational functions apply here.

Lemma 1.3 P'(z) exists and is holomorphic in $C - \Lambda$. Moreover,

$$P'(z) + 2/z^3 = 2a_2z + 4a_4z^3 + \dots$$

in a neighborhood of 0.

Proof: For holomorphic functions as we have defined them, the complex derivative always exists and equals the term-by-term differentiation of the original series at any point where it is expressed. \blacklozenge

1.5 The Differential Equation

In this subsection we'll establish the differential equation

$$(P')^2 = 4P^3 + g_2P + g_3. (9)$$

Lemma 1.4 In a neighborhood of 0 we have

$$P(z) = \frac{1}{z^2} + z^2 m_1(z);$$
 $P'(z) = \frac{-2}{z^3} + z m_2(z).$

Here m_1 and m_2 are holomorphic.

Proof: In view of the lemmas in the previous section, the functions

$$m_1(z) = a_2 + a_4 z^2 + \dots, \qquad m_2 = 2a_2 + 4a_4 z^2 + \dots$$

do the job. \blacklozenge

Using Lemma 1.4 we have

$$(P'(z))^2 = \frac{4}{z^6} - \frac{m_2(z)}{z^2}.$$
$$P^3(z) = \frac{1}{z^6} + \frac{3m_1(z)}{z^2} + 3m_1^2(z)z^2 + m_1^3(z)z^6.$$

Therefore

$$(P'(z))^2 - 4P^3(z) = \frac{m_3(z)}{z^2} + m_4(z).$$

Here m_3 and m_4 are functions which are holomorphic in a neighborhood of 0. For a suitable constant g_2 we therefore have

$$(P'(z))^2 - 4P^3(z) - g_2P(z) = m_5(z),$$

for some function m_5 which is holomorphic in a neighborhood of 0. Setting $g_3 = m_5(0)$ we have

$$(P'(z))^2 - 4P^3(z) - q_2P(z) - g_3 = m_6(z)$$

where $m_6(z)$ is holomorphic in a neighborhood of 0 and $m_6(0) = 0$.

Lemma 1.5 m_6 is identically 0.

Proof: For later reference, the argument we use is known as *the Maximum Principle*.

Note that m_6 is Λ periodic. Therefore, m_6 is is holomorphic in a neighborhood of every lattice point, and vanishes at every lattice point. Away from the lattice points, we know that m_6 is holomorphic. Hence m_6 is holomorphic on all of C and also Λ -invariant. It follows from compactness that $|m_6|$ achieves its max at some $z_0 \in C$.

If m_6 is not identically 0 then we can expand m_6 out in a nontrivial series about z_0 . There is some m such that

$$m_6(z) = m_6(z_0) + a_m(z - z_0)^m + higher order terms.$$

But for z very near z_0 the expression $a_m(z-z_0)^m$ is much larger than all other terms, and the map $z \to a_m(z-z_0)^m$ maps a small disk about z_0 to a small disk Δ about 0. But then m_6 maps a small disk about z_0 completely over a small disk containing $m_6(z_0)$. This contradicts the fact that $|m_6|$ achieves its max at z_0 .

Since m_6 is identically 0, we have

$$(P')^2 = 4P^3 + g_2P + g_3.$$

This is the Weierstrass differential equation, just as in Equation 1. We now define the map Ψ as in Equation 2. The rest of these notes are devoted to establishing the various nice properties of Ψ .

Remark: With a bit of effort, one can trace through the proof above and prove that

$$g_2 = \sum_{\lambda \neq 0} \frac{-60}{\lambda^4}; \qquad g_3 = \sum_{\lambda \neq 0} \frac{-140}{\lambda^6}.$$
 (10)

1.6 Holomorphic Maps

Let $P^2(C)$ be the complex projective plane. We say that a map

$$f: \boldsymbol{C} \to \boldsymbol{P}^2(\boldsymbol{C})$$

is holomorphic if for each $z \in C$ there is at least one of the 3 coordinate charts $\phi : \mathbf{P}^2(\mathbf{C})' \to \mathbf{C}^2$ such that the two coordinates of $\phi \circ f$ are holomorphic

functions. Here $\mathbf{P}^2(\mathbf{C})'$ denotes the subset of $\mathbf{P}^2(\mathbf{C})$ where the map ϕ is defined. Because the changes of coordinates (where defined) are themselves holomorphic map, this definition does not depend on which coordinate chart we use in the cases when there is more than one choice available.

We define Ψ as Equation 2. We regard the image of Ψ as lying in $P^2(C)$. That is

$$\Psi(z) = [P(z) : P'(z)) : 1], \tag{11}$$

for $z \notin \Lambda$ and $\Psi(z) = [0:1:0]$ for $z \in \Lambda$.

Lemma 1.6 Ψ is holomorphic on all of C.

Proof: Away from Λ both coordinates of Ψ are holomorphic. Therefore, by definition, Ψ is a holomorphic on $C - \Lambda$. It remains to understand what happens at points of Λ . We will use the coordinate chart in which we divide out by the second coordinate. The makes sense because Ψ maps lattice points to [0:1:0], the 'origin" of this chart, so to speak. Since Ψ is Λ -periodic it suffices to consider what happens at 0. We have

Consider the third coordinate:

$$\frac{1}{P'(z)} = \frac{1}{\frac{-2}{z^3} + 2a_2z + 4a_4z^3...} = \frac{(-1/2)z^3}{1+\Delta} = (-1/2)z^3(1-\Delta+\Delta^2-\Delta^3...),$$
$$\Delta = 2a_2z^4 + 4a_4z^6 + ...$$
(12)

When we expand this all out, we see that
$$1/P'(z)$$
 again equals a power series
in a neighborhood of 0. Similarly

$$\frac{P(z)}{P'(z)} = \frac{(-1/2)(z + a_2 z^3 + a_4 z^5 + a_6 z^7 \dots)}{1 + \Delta} = b_1 z + b_2 z^2 + b_3 z^3 \dots$$
(13)

which is just another series. We don't care about this series but we do note for later use that $b_1 = -1/2$, a nonzero number.

1.7 Surjectivity

Let \boldsymbol{E} be the elliptic curve. We have our map $\Psi : \boldsymbol{C}/\Lambda \to \boldsymbol{P}^2(\boldsymbol{C})$, but the image is contained in \boldsymbol{E} , so we may also write this as $\Psi : \boldsymbol{C}/\Lambda \to \boldsymbol{E}$.

In this section I'll prove that Ψ is surjective. Suppose not. Then there is some $g \in \mathbf{E}$ not in the image of Ψ . Let $T_g : \mathbf{E} \to \mathbf{E}$ be the map which is left multiplication by g^{-1} . That is, $T_g(h) = g^{-1} \oplus h$. Since the addition law is given by rational functions, the composition $\Phi = T_g \circ \Psi$ is again holomorphic. Since Ψ does not hit g, the new map Φ does not hit [0:1:0] the only "infinite point" on \mathbf{E} .

So, the image of Φ is contained entirely in \mathbb{C}^2 . The same Maximum Principle, used in Lemma 1.5, shows that the two coordinate functions of Φ , in these local coordinates, are constant. But if Φ is the constant map then so is Ψ . Given the series expansions above, this is certainly not the case. That contradiction finishes the proof.

1.8 Injectivity

We first show that Ψ is injective near 0. Using the same coordinates as in the proof of Lemma 1.6 we are reduced to showing that the series in Equation 13 is injective near 0. In other words, if the first coordinate is injective then of course the whole map is. The following lemma justifies this claim.

Lemma 1.7 The function $f(z) = b_1 z + b_2 z^2 + b_3 z^3 + ...$ is injective near 0 provided that $b_1 \neq 0$.

Proof: by scaling it suffices to prove this when $b_1 = 1$. We have f'(0) = 1. For z sufficiently near 0 f'(z) makes an angle of less than 1 degree with 1. Geometrically, if γ is any straight line segment sufficiently close to 0, then $f(\gamma)$ and γ make an angle of less than 1 degree. In other words, $f(\gamma)$ points almost in the same direction as γ . Now, if f(p) = f(q) we can join them by a line segment γ . On the one hand, $f(\gamma)$ has to start and end at f(p) and on the other hand, it stays with 1 degree of being a straight line segment. This is impossible.

Now we know that $\Psi : \mathbf{C}/\Lambda \to \mathbf{E}$ is injective when restricted to a sufficiently small neighborhood of 0. Furthermore, away from any neighborhood of 0 in \mathbf{C}/Λ , the coordinate functions of Ψ are bounded when viewed in the

usual local coordinates – i.e. dividing out by the third coordinate. So, if p is very near 0 and $\Psi(p) = \Psi(q)$, this last fact forces q to also lie very near 0. But then the local injectivity says that p = q. in short, if p is sufficiently close to 0, then there is no other point $q \neq p$ such that $\Psi(p) = \Psi(q)$.

Now we can finish the proof that Ψ is injective. Call a point $z \in C/\Lambda$ bad if there is some other point $w \in C/\Lambda$ such that $\Psi(z) = \Psi(w)$. From what we have just said there is some positive minimal distance between any bad point and 0. Let d be this minimal distance. Let $\{z_n\}$ be a sequence of bad points such that $||z_n|| \to d$. Let $\{w_n\}$ be points such that $\Psi(z_n) = \Psi(w_n)$. It may happen that $z_1 = z_2 = z_3$... That would be fine for the argument. Passing to a subsequence we can assume (by compactness) that $z_n \to z$ and $w_n \to w$. There are several cases to consider.

Case 1: Suppose $z \neq w$. Then z is bad and $\Psi(z) = \Psi(w)$. Let $p = \Psi(z)$ and let L_p be the line tangent to E at p. We have a projection map π which maps a neighborhood of p in E into L_p . This map is injective and the composition $\pi \circ \Psi$ is holomorphic. We pick p to be the origin in L_p so that $\pi \circ \Psi(z) = 0$. There is some $m \geq 1$ such that

$$\pi \circ \Psi(z') = a_m (z' - z)^m + \text{higher order terms}$$
(14)

for z' sufficiently near z.

When |z' - z| is sufficiently small, this first term dominates, and $\pi \circ \Psi$ maps a small circle centered at z to a loop which winds m times around 0. But then, just as in the winding number proof of the Fundamental Theorem of Algebra, $\pi \circ \Psi$ maps a small disk centered at 0 onto an open neighborhood of 0. But all the same may be said for $\pi \circ \Psi$ acting in a small disk about w. The images of the two small disks intersect in an open set containing 0. This shows that all points sufficiently close to z are bad. Some of these points are closer to 0 than z, and we have a contradiction.

Case 2: Suppose z = w. We make the same constructions as in Case 1. This time we have $m \ge 2$ in Equation 14 because otherwise we contradict Lemma 1.7. This means that $\pi \circ \Psi$ maps a small circle centered about z to a curve which is nearly circular and winds m times around 0. But from this picture, we see that each point sufficiently near 0 has m pre-images under $\pi \circ \Psi$ and these points nearly make a regular m-gon about 0. Hence all points sufficiently near p are bad. Again, we have a contradiction.

1.9 The Inverse Map

At this point we know that $\Psi : \mathbf{C}/\Lambda \to \mathbf{E}$ is a holomorphic bijection. It remains to see that the inverse map $\Psi^{-1} : \mathbf{E} \to \mathbf{C}/\Lambda$ is holomorphic. Technically, \mathbf{E} is not a subset of \mathbf{C} , so we need to expand our idea of what this means.

In the previous section we discussed a number of local coordinate systems of the form $\pi: \mathbf{E} \to L_p$ where L_p is a tangent line to \mathbf{E} . In local coordinates, these maps are just linear projections. Moreover, at least for a neighborhood of 0, the map π^{-1} is well-defined. When we say that Ψ^{-1} is holomorphic, we mean that $\Psi^{-1} \circ \pi^{-1}$ is a holomorphic map from an open set of \mathbf{C} to \mathbf{C}/Λ . This makes sense because we can identify small open sets in \mathbf{C}/Λ with open subsets in \mathbf{C} . In short, if we work entirely in local coordinate systems, the notion of a holomorphic from \mathbf{E} to \mathbf{C}/Λ just boils down to the series definition given above.

Choose some $z_0 \in C/\Lambda$ and consider $f(z) = \pi \circ \Psi(z)$ for z in a neighborhood of z_0 . Since f is holomorphic we can write

$$f(z) = a_0 + a_1(z - z_0) + a_2(z - z_0)^2 + \dots$$

We can arrange, as above, that $a_0 = 0$. If $a_1 = 0$ then the same argument as in Case 2 of the previous section shows that f is not injective. Since this is false, $a_1 \neq 0$. In short

$$f(z) = a_1(z - z_0) +$$
higher order terms.

Note that $f'(z_0)$ is nonzero, and this is true at all points in the domain.

There are various ways to show that f^{-1} is holomorphic, depending on which definition of *holomorphic* is used. The traditional definition of a holomorphic function is that its complex derivative exists at each point. Thanks to term-by-term differentiation, convergent power series are traditionally holomorphic, and indeed have complex derivatives of all orders. The following lemma is tailor made to our situation.

Lemma 1.8 Suppose U and V are open subsets of the plane and $f: U \to V$ is a bijection given by a convergent power series. Then f^{-1} has complex derivatives of all orders, and all partial derivatives of f^{-1} exist.

Proof: The same argument as above shows that f' never vanishes in U. We first show that f^{-1} has a complex derivative. By translating we can assume

that the point where we are trying to establish the existence of g' is 0, and f(0) = 0. Let $g = f^{-1}$. We will show that g has a complex derivative at 0. Replacing f by a complex multiple, we can assume that f'(0) = 1. This means that at small scales f is near the identity near 0. Here is another way to put this. Let D_n denote dilation by n. That is, $D_n(z) = nz$. Since f'(0) = 0 the map $D_n \circ f \circ D_{1/n}$ converges to the identity map on all of C as $n \to \infty$. But the inverse of $D_n \circ f \circ D_{1/n}$ then also converges to the identity map. The inverse of $D_n \circ f \circ D_{1/n}$ is of $D_n \circ g \circ D_{1/n}$. Therefore, of $D_n \circ g \circ D_{1/n}$ converges to the identity on C. Therefore g' exists at 0 and g'(0) = 1.

Now we can apply the chain rule:

$$1 = (f \circ g)'(z) = f'(g(z))g'(z).$$

Rearranging, we have the

$$g' = \frac{1}{f' \circ g}.$$

Since g and f' both have complex derivatives, $f' \circ g$ has a complex derivative by the chain rule. But then $1/(f' \circ g)$ has a complex derivative by the chain rule. Hence g' has a complex derivative. But this means that g has 2 complex derivatives. Repeating the argument, we see that g has 3 complex derivatives, and so on.

So, our map Ψ is a bi-holomorphism in the sense that, in local coordinates, both Ψ and Ψ^{-1} have complex derivatives of all orders.

Remarks:

(i) Convergent power series, conidered as maps of \mathbf{R}^2 , have derivatives of all orders in the real sense. The same kind of argument as above then establishes that the inverse of a convergent power series has real partial derivatives of all orders. In particular, the mixed partials commute, something we will use below.

(ii) The reader who knows some complex analysis should be able to use the Cauchy integral formula to prove that a function with complex derivatives of all orders equals its own Taylor series in a neighborhood of each point. That is, the inverse of a convergent power series is also a convergent power series.

1.10 Group Isomorphism

Now we will show that $\Psi : C/\Lambda \to E$ is a group isomorphism. We need one more result from complex analysis.

Lemma 1.9 A bounded and Λ -periodic holomorphic function is constant.

Proof: Let f be the function under consideration. If we know that f equals a power series in the neighborhood at each point, then this is exactly the argument from Lemma 1.5, namely the Maximum Principle.

However, given the route we took in the last section, we should really give a proof that only depends on f having complex derivatives of all orders. Write f = u + iv, where u and v are real valued functions. The fact that f has a complex derivative means that $u_x = v_y$ and $u_y = -v_x$. Here $u_x = \partial u/\partial x$, etc. These equations are known as the Cauchy-Riemann equations. Hence

$$u_{xx} + u_{yy} = v_{xy} - v_{xy} = 0. (15)$$

In Equation 15 we used the fact that the mixed partials commute.

Equation 15 says that u is a *harmonic function* It follows from Green's Theorem that the value of u at each point equals the average of u on a disk centered at that point. But then u cannot have an interior maximum and we get the same contradiction as in Lemma 1.5 unless u is constant. The same argument shows that v is constant.

We want to show that $\Psi(a + b) = \Psi(a) + \Psi(b)$ for any $a, b \in \mathbb{C}/\Lambda$. Let $A = \Psi(a)$ and $B = \Psi(b)$. Let $T_A : \mathbb{E} \to \mathbb{E}$ denote addition by A. This is a holomorphic map of E. Define

$$\tau_A = \Psi^{-1} \circ T_A \circ \Psi \tag{16}$$

Lemma 1.10 τ_A is a translation.

Proof: T_A is a holomorphic map of \boldsymbol{E} . At the same time, T_A is a homeomorphism with no fixed points. Hence τ_A is a holomorphic homeomorphism of \boldsymbol{C}/Λ with no fixed points. Let $\tau = \tau_A$. We have the quotient map $\pi : \boldsymbol{C} \to \boldsymbol{C}/\Lambda$. Let $g = \pi \circ \tau : \boldsymbol{C} \to \boldsymbol{C}/\Lambda$. The derivative g' makes sense as a map from $\boldsymbol{C} \to \boldsymbol{C}$. Since g' is continuous and Λ -periodic, there is some M such that |g'| < M. But then g' is both bounded and holomorphic. Hence

g' is constant. Hence τ' is constant. Since τ preserves the area of C/Λ , we must have $|\tau'| = 1$. If τ had any rotational component, it would have a fixed point. Hence $\tau' = 1$. This implies that τ is a translation.

We have

$$\tau_A(0) = \Psi^{-1} \circ T_A \circ \Psi(0) = \Psi^{-1} \circ T_A([0:1:0]) = \Psi^{-1}(A) = a.$$
(17)

Likewise $\tau_B(0) = b$. Since τ_A is a translation and $\tau_A(0) = a$,

$$\tau_A(b) = a + b. \tag{18}$$

But then

$$\tau_A \circ \tau_B(0) = \tau_A(b) = a + b. \tag{19}$$

On the other hand.

$$\tau_A \circ \tau_B(0) = (\Psi^{-1} \circ T_A \circ \Psi) \circ (\Psi^{-1} \circ T_B \circ \Psi)(0) =$$
$$\Psi^{-1} \circ T_A \circ T_B \circ \Psi(0) =$$
$$\Psi^{-1} \circ T_A \circ T_B([0:1:0]) = \Psi^{-1}(A+B).$$

In short

$$a + b = \tau_A \circ \tau_B(0) = \Psi^{-1}(A + B)$$
 (20)

Applying Ψ , we see that $\Psi(a+b) = \Psi(a) + \Psi(b)$, as claimed.