The goal of these notes is to explain Weierstrass Uniformization.

1 Lattices

Say that 2 complex numbers α and β are *independent* of α/β is not real. For instance 1 and i are independent.

A *lattice* in $\boldsymbol{C}$ is a set of points of the form

$$\Lambda = \{m\alpha + n\beta \quad m, n \in \boldsymbol{Z}\}, \tag{1}$$

where α and β are independent numbers. The set of points in Λ forms a grid of parallelograms. The classic case is when $\alpha = 1$ and $\beta = i$. In this case $\Lambda = \boldsymbol{Z}[i]$, the Gaussian integers.

The quotient $\boldsymbol{C}/\Lambda$ has several nice properties.

1. $\boldsymbol{C}/\Lambda$ is homeomorphic to a torus – namely, a single parallelogram with its sides identified.

2. $\boldsymbol{C}/\Lambda$ abelian group under addition, since both $\boldsymbol{C}$ and Λ are abelian groups under addition.

A map $f : \Lambda \to \boldsymbol{C}$ is called Λ-*periodic* if $f(\lambda + z) = f(z)$ for all $z \in \boldsymbol{C}$ and all $\lambda \in \Lambda$. In this case, f induces a map from $\boldsymbol{C}/\Lambda$ into $\boldsymbol{C}$. This new map is usually also denoted by f. We can also talk about Λ-periodicity when f is not defined at all points of $\boldsymbol{C}$. In the case of interest, we will be able to interpret f as a map from $\boldsymbol{C}$ to $\boldsymbol{C} \cup \infty$.

2 The Weierstrass Function

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

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

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 2 wants to be. Here is the definition.

$$P(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \frac{2z\lambda - z^2}{\lambda^2 (z - \lambda^2)}. \tag{3}$$

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

$$\left| \frac{z^2 - 2z\lambda}{\lambda^2(z-\lambda^2)} \right| < \frac{C_z}{|\lambda|^3}. \tag{4}$$

Here C_z is a constant that depends on z in a way that we don't care about. The series in Equation 3 does converge because the corresponding series

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

converges.

The Weierstrass function $P(z)$ is defined for all $z \in \boldsymbol{C} - \Lambda$. As $z \to \lambda \in \Lambda$, the quantity $|P(z)|$ tends to ∞. One says that $P(z)$ has *poles* at points of Λ.

3 Differentiability

In this section we'll prove that the function P is complex analytic on $\boldsymbol{C} - \Lambda$ and that

$$P'(z) = \sum_{\lambda \in \Lambda} \frac{-2}{(z-\lambda)^3}, \qquad \forall z \in \boldsymbol{C} - \Lambda. \tag{5}$$

This is the standard proof that term-by-term differentiation works.

For any N we can write $P = P_N + R_N$, where

$$P_N(z) = \frac{1}{z^2} + \sum_{0 < |\lambda| < N} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right). \tag{6}$$

and R_N is the remainder. In other words, P_N is defined just like P, except we only sum over the lattice points inside the disk of radius N.

Since P_N just involves a finite number of terms, we have

$$dP_N/dz = \lim_{h \to 0} \frac{P_N(z+h) - P_N(h)}{h} = \sum_{|\lambda| < N} \frac{-2}{(z-\lambda)^3} \tag{7}$$

Note that the case $\lambda = 0$ is included in the sum.

To understand what happens to the remainder, we write

$$R_N = \sum_{|\lambda \geq N} f_\lambda(z); \qquad f_\lambda(z) = \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}. \tag{8}$$

We have

$$\frac{f_\lambda(z+h) - f_\lambda(z)}{h} = \frac{2\lambda - h - 2z}{(z-\lambda)^2(z-\lambda-h)^2}. \tag{9}$$

For now on, we suppose $|h| < 1$. Also, we fix z. Once $|\lambda|$ is large ebough we have

$$\left|\frac{f_\lambda(z+h) - f_\lambda(z)}{h}\right| < \frac{C_z}{|z-\lambda|^3}. \tag{10}$$

Again, the constant C_z depends on z in a way that we don't care about. For any $\epsilon_1 > 0$ we can choose N large enough so that

$$\left|\frac{R_N(z+h) - R_N(z)}{h}\right| < C_z \sum_{|\lambda \geq N} \frac{1}{|z-\lambda|^3} < \epsilon_1. \tag{11}$$

From Equation 11 we have

$$\begin{aligned} \left|\frac{P(z+h) - P(z)}{h} - \sum_\lambda \frac{-2}{(z-\lambda)^3}\right| \leq \\ \epsilon_1 + \left|\frac{P_N(z+h) - P_N(z)}{h} - \sum_\lambda \frac{-2}{(z-\lambda)^3}\right| \leq \\ \epsilon_1 + \epsilon_2 + \left|\frac{P_N(z+h) - P_N(z)}{h} - \sum_{|\lambda| < N} \frac{-2}{(z-\lambda)^3}\right| \leq \\ \epsilon_1 + \epsilon_2 + \epsilon_3 \end{aligned} \tag{12}$$

The terms ϵ_1 and ϵ_2 tend to 0 as $N \to \infty$, and the term ϵ_3, which comes from Equation 7, tends to 0 as $h \to 0$. This proves that

$$\lim_{h \to 0} \left|\frac{P(z+h) - P(z)}{h} - \sum_\lambda \frac{-2}{(z-\lambda)^3}\right| = 0. \tag{13}$$

4 The Differential Equation

In this section we'll establish the differential equation

$$(P')^2 = 4P^3 + g_2 P + g_3. \tag{14}$$

A function f is called *even* if $f(-z) = f(z)$ for all z. Also, f is called *odd* if $f(-z) = -f(z)$ for all z.

Lemma 4.1 *P is even and Λ-periodic.*

Proof: Since $1/z^2$ is even, it suffices to prove that $Q(z) = P(z) - 1/z^2$ is even. Since P' is odd, so is Q'. Also, $Q(0) = 0$. Since Q' is odd and $Q(0) = 0$, we get that Q is even. Hence P is even.

Now we show periodicity. Let $\lambda \in \Lambda$ be any point. Let $Q(z) = P(z+\lambda) - P(z)$. From Equation 5 we see that $P'(z)$ is clearly Λ-periodic. Therefore $Q'(z) = 0$. Hence $Q(z) = C_\lambda$, a constant that perhaps depends on λ. We just have to show that $C_\lambda = 0$. But

$$C_\lambda = P(-\lambda/2 + \lambda) - P(-\lambda/2) = P(\lambda/2) - P(-\lambda/2) = 0,$$

since P is even. ♠

Lemma 4.2 *In a neighborhood of 0 we have*

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

Here m_1 and m_2 are CA in a neighborhood of 0.

Proof: Let $Q(z) = P(z) - 1/z^2$. $Q(z)$ is even and $Q(0) = 0$. Since $Q(0) = 0$ and Q is CA, the quotient $Q(z)/z$ is bounded in a neighborhood of 0. So, we can write $Q(z) = zR(z)$ where $R(z)$ is CA in a neighborhood of 0. Note that $R(z)$ is odd. Hence $R(0) = 0$. The same argument now shows that $R(z) = z m_1(z)$. Hence $Q(z) = z^2 m_1(z)$. This gives the first equation. The second equation comes from differentiating the first one. ♠

Lemma 4.2 tells us that

$$A(z) = 4P^3 - g_2 P - g_3 - (P')^2 = \frac{m_3(z) + g_2}{z^2} + g_3 + m_4(z), \tag{15}$$

where m_3 and m_4 are CA in a neighborhood of 0. We choose g_2 so that $m_3(0) + g_2 = 0$. We choose g_3 so that A vanishes at some point.

Lemma 4.3 *$A(z)$ is bounded in a neighborhood of 0.*

Proof: Consider the function $q(z) = m_3(z) + q_2$. Is suffices to prove that $q(z)/z^2$ is bounded in a neighborhood of 0. The function $q(z)$ is even and $q(0) = 0$. The same argument as in Lemma 4.2 shows that $q(z) = z^2 s(z)$, where $s(z)$ is CA in a neighborhood of 0. This does it. ♠

The function $A(z)$ is Λ-periodic. Hence $A(z)$ is bounded in a neighborhood of each lattice point. On the other hand, $A(z)$ is CA in $\boldsymbol{C} - \Lambda$. So, A is bounded in the complement of any neighborhood of Λ. Hence A is bounded. All the singularities of A are removable, so A extends to a bounded CA function on $\boldsymbol{C}$. But then A is constant. Our choice of g_3 gives $A = 0$. This establishes Equation 14.

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

$$g_2 = \sum_{\lambda \neq 0} \frac{-60}{\lambda^4}; \qquad g_3 = \sum_{\lambda \neq 0} \frac{-140}{\lambda^6}. \tag{16}$$

5 Map to the Elliptic Curve

Let E be the elliptic curve

$$y^2 = 4x^3 + g_2 x + g_3. \tag{17}$$

We will assume that this elliptic curve is nonsingular, meaning that

$$4g_2^3 + 27g_3^2 \neq 0.$$

In fact, all choices of Λ have this property, but this is a bit of a digression to prove.

There is a map from $\boldsymbol{C}$ into E, given by

$$\Psi(z) = (P(z), P'(z)). \tag{18}$$

Equation 14 tells us that this map actually lands in E. When $z \in \Lambda$, we define $\Psi(z) = [0:1:0]$, the infinite point.

Since Ψ is Λ-periodic, Ψ induces a map (with the same name)

$$\Psi : \boldsymbol{C}/\Lambda \to E. \tag{19}$$

The map Ψ is called the *Weierstrass uniformizing map*.

6 Branch Points

As a prelude to understanding the map Ψ, we need some information about the derivatives of P. A *branch point* of P is a point z such that $P'(z) = 0$. In this section we characterize the branch points. Let $\frac{1}{2}\Lambda$ denote the set of points of the form $\lambda/2$ where $\lambda \in \Lambda$. Let $\Lambda' = \frac{1}{2}\Lambda - \Lambda$. We will prove:

- $P'(z) = 0$ if $z \in \Lambda'$.
- $P'(z) = 0$ only if $z \in \Lambda'$.
- $P''(z) \neq 0$ if $z \in \Lambda'$.

Suppose that $z \in \Lambda'$. Then

$$P(z+h) = P(z+h-2z) = P(-z+h) = P(z-h). \tag{20}$$

The first equality comes from the fact that $2z \in \Lambda$ and that P is Λ-periodic. The last equality comes from the fact that Λ is even. Since P' is continuous,

$$2P'(z) = \lim_{h \to 0} \frac{P(z+h) - P(z-h)}{h} = 0.$$

It is convenient to define $Q = P'$. Suppose that $Q(a) = 0$. We can write $Q(a+z) = z^m g(z)$, where $g(0) \neq 0$ and m is some integer. We define m to be the *multiplicity* of a. This notion of multiplicity coincides with the notion of the multiplicity of a root of a polynomial. If both $Q(a)$ and $Q'(a)$ are 0 then a has multiplicity greater than 1. So, either of the remaining claims above fails, the equation $Q = 0$ has at least 4 solutions in $\boldsymbol{C}/\Lambda$, counting multiplicity.

The multiplicity has the following topological interpretation. Suppose that C is a loop that surrounds a and no other roots of Q. Then the multiplicity of a counts the number of times $Q(C)$ winds around 0. More generally, if C is a loop that surrounds the roots $a_1, ..., a_k$ of Q, then the sum of multiplicities of $a_1, ..., a_k$ counts the number of times $Q(C)$ winds around 0. The multi-root case can be deduced from the single root case by considering pictures of the kind shown in Figure 1. The idea is that the winding number of the outer loop, the loop we care about, is the same as the winding number of the inner loop, and the winding number of the inner loop is the sum of the winding numbers of the 3 small loops surrounding the individual roots.

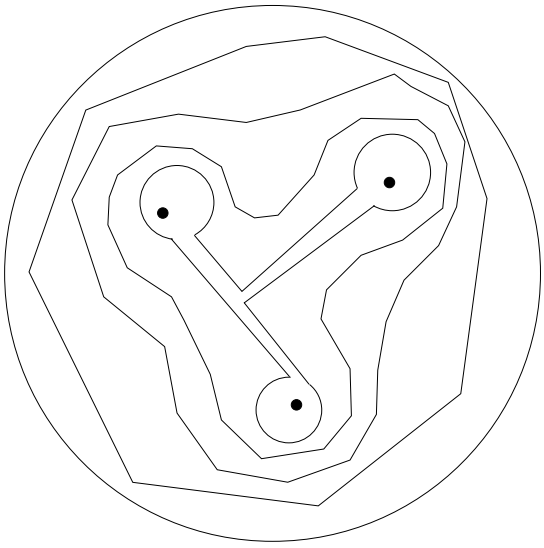

Figure 1.

For any $u \in \boldsymbol{C}$ we define $N(u)$ to be the number of solutions to the equation $Q(z) - u = 0$, counting multiplicity. We suppose that $N(0) \geq 4$. By Equation 5, we have

$$Q(z) = \frac{1}{z^3} + g(z),$$

where $g(z)$ is CA in a neighborhood of 0. From this equation we see that $Q(z) - u = 0$ only has solutions near lattice points when $|u|$ is large, and moreover that $N(u) = 3$ when $|u|$ is large.

It follows from the topological interpretation of multiplicity that the function $u \to N(u)$ varies continuously. On the other hand, this function is integer-valued. Hence, it is impossible for $N(0) > 3$. This is a contradiction. This completes our proofs of the claims.

7 Regularity of the Map

In this section we will show that Ψ is a regular map. This is to say that Ψ' never vanishes. First, suppose that $z \in \boldsymbol{C} - \Lambda$. We have $\Psi'(z) = (P'(z), P''(z))$. Note that $P'(z)$ and $P''(z)$ are not both zero, by the result in §6.

It remains to consider the case when $z \in \Lambda$. Since Ψ is Λ-periodic, it suffices to consider the case $z = 0$. The secret in this case is to change

coordinates to that we are still dealing with a map into $\boldsymbol{C}^2$. We can't use the usual copy of $\boldsymbol{C}^2$ sitting inside $P^2(\boldsymbol{C})$, so we will use one of the other copies. We have $\Psi(0) = [0:1:0]$. To analyze the derivative, we consider the picture in the plane $\boldsymbol{C}^2$ consisting of points $y = 1$. For points $z \in \boldsymbol{C}$ near 0,

$$\Psi(z) = [P(z), P'(z) : 1] = [P(z)/P'(z) : 1 : 1/P'(z)].$$

Consider the first coordinate, $g(z) = P(z)/P'(z)$. From Lemma 4.2, the function $g(z)$ is bounded in a neighborhood of 0. Also, $\lim_{z\to 0} |g(z)| = 0$. So, we can write $g(z) = zh(z)$. If $h(0) = 0$ then $g(z) = z^2 m(z)$, where $m(z)$ is CA in a neighborhood of 0. This contradicts Lemma 4.2. So, $h(0) \neq 0$. But then $g'(0) \neq 0$. Hence $\Psi'(0) \neq 0$.

8 Surjectivity of the Map

Now we'll show that $\Psi : \boldsymbol{C}/\Lambda \to E$ is onto. Be warned that this section requires a bit of background in real analysis. The main result we will use is that a nonempty subset of E, which is both open and closed, must be all of E. This follows from the fact that E is connected. Obviously $\Psi(\boldsymbol{C}/\Lambda)$ is nonempty. So, we just need to show that this set is open and closed.

Closed: This follows from the fact that $\boldsymbol{C}/\Lambda$ is compact, and Ψ is continuous. The continuous image of a compact set is always closed. Here is a more elementary argument, which explains the meaning of "compactness". Choose some point w that lies in the closure of $\Psi(\boldsymbol{C}/\Lambda)$. By definition, there is a sequence $\{z_i\}$ in $\boldsymbol{C}/\Lambda$ such that $\Psi(z_i)$ converges to w. Since $\boldsymbol{C}/\Lambda$ is compact, we can pass to a subsequence so that $\{z_i\}$ is a convergent subsequence. Let $z = \lim z_i$. By continuity $\Psi(z) = w$. Hence $w \in \Psi(\boldsymbol{C}/\Lambda)$. Since w was an arbitrary point in the closure of $\Psi(\boldsymbol{C}/\Lambda)$, we see that $\Psi(\boldsymbol{C}/\Lambda)$ contains its closure. Hence $\Psi(\boldsymbol{C}/\Lambda)$ is closed.

Open: Let $a \in \boldsymbol{C}$. Let L be the tangent line to E at a. Let π be the projection map from E onto L. Since E is a nonsingular elliptic curve, π is a local homeomorphism from a neighborhood of $\Psi(a)$ in E to an open set in L.

Consider the auxilliary map

$$\pi \circ \Psi : \boldsymbol{C} \to L.$$

This is a C.A. map from $\boldsymbol{C}$ to L, and L is just a copy of $\boldsymbol{C}$. The map $\pi \circ \Psi$ is C.A. Since Ψ is regular, the derivative of $\pi \circ \Psi$ does not vanish at a. Hence, $\pi \circ \Psi$ is a local homeomorphism. Hence $\pi \circ \Psi$ maps an open neighborhood U of a in $\boldsymbol{C}$ onto an open neighborhood of $\pi \circ \Psi(a)$ in L. Given what we have already said about π, we see that $\Psi(U)$ is an open set in E which contains $\Psi(a)$. This shows that every point of $\Psi(\boldsymbol{C})$ is contained in an open subset of $\Psi(\boldsymbol{C})$. Hence $\Psi(\boldsymbol{C})$ is open in E.

Remark: We actually didn't need to know that Ψ is a regular map. It always happens that the image of an open set under a non-trivial CA map is open.

9 Injectivity of the Map

Here we will show that Ψ is injective. Let $X \subset \boldsymbol{C}/\Lambda$ denote those points where Ψ is not injective. That is, each $a \in X$ is such that there is some distinct $b \in X$ such that $\Psi(a) \neq \Psi(b)$. Note that $[0] \notin X$ since $[0]$ is the only point of $\boldsymbol{C}/\Lambda$ which Ψ maps to the line at infinity. So, X is not all of $\boldsymbol{C}/\Lambda$. We will show that X is both open and closed. Since $\boldsymbol{C}/\Lambda$ is connected, this shows that X is empty!

Closed: Suppose a lies in the closure of X. Let $\{a_n\}$ be a sequence in X converging to a. Let $\{b_n\}$ be a sequence so that $\Psi(a_n) = \Psi(b_n)$. Passing to a subsequence, we can assume that $b_n \to b$. By continuity, we have $\Psi(a) = \Psi(b)$. We just have to prove that $a \neq b$. Since Ψ is regular, Ψ is a homeomorphism from a neighborhood U of a into E. The restriction of Ψ to U is injective. But $a_n \in U$ for n large. Hence $b_n \notin U$ for n large. Hence $b \notin U$. Hence $a \neq b$. This proves that $a \in X$. Hence X is closed.

Open: Suppose that $a \in X$. Let $b \in X$ be such that $\Psi(a) = \Psi(b)$ and $a \neq b$. Since Ψ is regular, there are small disks U_a and U_b about a and b such that $\Psi(U_a)$ and $\Psi(U_b)$ are both open sets containing the common point $w = \Psi(a) = \Psi(b)$. We can take U_a and U_b so small that they are disjoint, and we can shrink U_a to be so small that $\Psi(U_a) \subset \Psi(U_b)$. But then $U_a \subset X$. Hence X contains an open set which contains a. Since a was an arbitrary point of X, this shows that X is open.

10 Crash Course on Riemann Surfaces

It only remains to show that Ψ is a group isomorphism. Before we do this, we need to make a little digression. We would like to say when a map $f : E \to E$ is complex analytic. This doesn't quite make sense, because E is not really $\boldsymbol{C}$. However, E is nonsingular, and there is a projection from E to each of its tangent planes. We will use these projections to talk about CA maps of E. Essentially, we are treating E as a Riemann surface, but we are doing to do it without making a big fuss about a formal definition of a Riemann surface.

Given $a \in E$ let $\pi_a : E \to L$ be the projection from E to the tangent line at a. We have already considered these maps. Suppose that $\phi : E \to E$ is a map of E and $b = \phi(a)$. We say that f is CA at a if

$$\pi_b \circ f \circ \pi_a^{-1} \tag{21}$$

is CA in a neighborhood of $\pi_a(a)$. The map π_a^{-1} makes sense at least in a neighborhood of $\pi_a(a)$.

Lemma 10.1 *$f : E \to E$ is CA if and only if $\Psi^{-1} \circ f \circ \Psi$ is a CA map of $\boldsymbol{C}/\Lambda$.*

Proof: The point is that the coordinates of Ψ are CA maps. So, this is just an exercise in the chain rule. ♠

Here is the main example of interest to us. Let $T_A : E \to E$ denote addition by A. That is $T_A(P) = A + P$ for all $P \in E$.

Lemma 10.2 *T_A is a CA map of E.*

Proof: Recall that there are rational functions describing the group law on E. Hence, the coordinates of T_A are rational functions. The compositions in Equation 21 are rational functions on $\boldsymbol{C}$. (Here we are thinking of the tangent lines as copies of $\boldsymbol{C}$.) Hence, the compositions in Equation 21 are all CA. So, by definition T_A is CA. ♠

11 Group Isomorphism

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

$$\tau_A = \Psi^{-1} \circ T_A \circ \Psi \tag{22}$$

Lemma 11.1 *τ_A is a translation.*

Proof: T_A is a CA map of E. At the same time, T_A is a homeomorphism with no fixed points. Hence τ_A is a CA homeomorphism of $\boldsymbol{C}/\Lambda$ 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 CA. Hence g' is constant. Hence τ' is constant. Since τ preserves the area of $\boldsymbol{C}/\Lambda$, 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

$$\tau_A(0) = \Psi^{-1} \circ T_A \circ \Psi(0) = \Psi^{-1} \circ T_A([0:1:0]) = \Psi^{-1}(A) = a. \tag{23}$$

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

$$\tau_A(b) = a + b. \tag{24}$$

But then

$$\tau_A \circ \tau_B(0) = \tau_A(b) = a + b. \tag{25}$$

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

$$a + b = \tau_A \circ \tau_B(0) = \Psi^{-1}(A + B) \tag{26}$$

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