Math 213a: Complex analysis
Notes on doubly periodic functions

Lattices. Let V be a real vector space of dimension n. A subgroup $L \subset V$ is said to be a *lattice* if it satisfies one of the following equivalent conditions:

i) L is the subgroup generated by a basis of V.
ii) There exists an invertible linear transformation $A : \mathbf{R}^n \to V$ such that $L = A(\mathbf{Z}^n)$.
iii) L is discrete and has rank n.
iv) L is discrete and has rank at least n.
v) L is co-compact and has rank n.
vi) L is co-compact and has rank at most n.
vii) L is discrete and co-compact.

For example, $\mathbf{Z}^n$ is a lattice in $\mathbf{R}^n$, and indeed (ii) says that all lattices are linearly equivalent to $\mathbf{Z}^n \subset \mathbf{R}^n$. As usual, notions like "discrete" make sense because all norms on a finite-dimensional real vector space are equivalent. Also, "co-compact" means that the quotient space $V/\overline{L}$ is compact, where $\overline{L}$ is the closure of L (which coincides with L when L is discrete); the map of (ii) then induces an identification of this quotient space with the n-torus $\mathbf{T}^n = \mathbf{R}^n/\mathbf{Z}^n = (\mathbf{R}/\mathbf{Z})^n$. By a standard Heine-Borel argument, for each norm $|\cdot|$ on V the co-compactness of L is equivalent to the existence of R such that for each $x \in V$ there exists $v \in L$ such that $|x - v| < R$; that is, such that balls of radius R about L cover V.

The equivalence of these various conditions is a reasonably easy exercise. Probably the only tricky part is proving that a discrete subgroup $L \subset V$ has rank at most n. To do this, we may argue as follows. Suppose $v_1, \ldots, v_{n+1} \in L$. Fix a norm $|\cdot|$ on V, and let $C = \sum_{j=1}^{n+1} |v_j|$. For any integer M, the lattice contains all the linear combinations $\sum_{j=1}^{n+1} a_j v_j$ with each $a_j \in \{0, 1, 2, \ldots, M-1\}$. Each of these has norm $< CM$, so all are contained in a ball of volume $O(M^n)$. There are M^{n+1} such vectors, so by a pigeonhole argument two of them, say $v = \sum_{j=1}^{n+1} a_j v_j$ and $v' = \sum_{j=1}^{n+1} a_j v'_j$, are contained in a cube of side $O(1/M)$. Hence $|v - v'| \ll 1/M$. But $v - v' \in L$. Thus if M is large enough then $0 = v - v' = \sum_{j=1}^{n+1} (a_j - a'_j) v_j$. We have thus found a nontrivial $\mathbf{Z}$-linear relation among the v_j. Alternatively, we may use induction on n. Then if L has rank at least n, any n lattice vectors that are $\mathbf{Z}$-linearly independent must also be $\mathbf{R}$-linearly independent, and thus generate a lattice $L' \subseteq L$. Then L/L' is a discrete subgroup of the torus V/L'. But this torus is compact, so any discrete subset is finite. Therefore L and L' have the same rank, and this completes the induction step and the proof.

We shall need the following elementary estimate:

Lemma 1. *Let V be a real vector space of dimension n. For any lattice $L \subset V$ and any norm $|\cdot|$ on V, there exist positive constants A, B such that for all*

$R > 0$ the ball $B_R := \{v \in V : |v| < R\}$ contains at least AR^n lattice vectors and at most BR^n nonzero lattice vectors.

Proof: By (ii) we may assume that $(V, L) = (\mathbf{R}^n, \mathbf{Z}^n)$. By equivalence of norms there exist positive constants α, β such that $\alpha|v|_\infty \leq |v| \leq \beta|v|_\infty$ for all $v \in \mathbf{R}^n$. It is thus enough to prove the lemma for the norm $|\cdot|_\infty$. But for this norm B_r contains exactly $(2\lfloor R \rfloor + 1)^n$ lattice vectors. □

[In fact one can give a more precise estimate: $\#(B_R \cap \mathbf{Z}^n)$ is asymptotic to $R^n \operatorname{Vol}(B_1)$ as $R \to \infty$. This can be obtained by considering $R^{-n}\#(B_R \cap \mathbf{Z}^n)$ as a Riemann sum for the integral over $\mathbf{R}^n$ of the characteristic function of B_1. One readily obtains the error estimate $\#(B_R \cap \mathbf{Z}^n) - R^n \operatorname{Vol}(B_1) \ll R^{n-1}$; the example of the norm $|\cdot|_\infty$ shows that in general one cannot do better. The size of the error for other norms, such as the Euclidean norm $|\cdot|_2$, is a famous open problem, even for $n = 2$.]

Corollary. *For $n, V, |\cdot|, L$ as in Lemma 1, the sum of $|v|^{-s}$ over nonzero $v \in L$ converges if and only if $s > n$.*

Proof: This is an exercise in partial summation. □

A basis $v_1, \ldots, v_n$ for V determines a lattice $L = \mathbf{Z}v_1 \oplus \mathbf{Z}v_2 \oplus \cdots \oplus \mathbf{Z}v_n$. A given lattice can be obtained from many bases. In general, two bases $v_1, \ldots, v_n$ and $v'_1, \ldots, v'_n$ generate the same lattice if and only if they are related by a linear transformation in $\mathrm{GL}_n(\mathbf{Z})$. Note that an $n \times n$ matrix M is in $\mathrm{GL}_n(\mathbf{Z})$ if and only if both M and M^{-1} have integer entries; equivalently (using the formula for M^{-1} in terms of the adjoint matrix), if and only if M has integer entries and determinant ± 1. [For a general commutative ring A, the same argument shows that $\mathrm{GL}_n(A)$ consists of the square matrices M of size n with entries in A such that $\det(M)$ is invertible in A.] Once we choose a basis for L, we may identify $\mathrm{GL}_n(\mathbf{Z})$ with the group automorphisms of L, or the (necessarily invertible) linear maps $T : V \to V$ such that $T(L) = L$. We may then identify the space of lattices in V with the quotient space $\mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z})$.

We now put more structure on V. First choose a volume form, a.k.a. a generator e of the 1-dimensional vector space $\wedge^n V$. Then the torus V/L inherits a volume form, and being compact has a finite volume, which is an invariant of L called its *covolume* and often denoted by $|L|$. We readily see that the covolume is given by the formula

$$v_1 \wedge v_2 \wedge \cdots \wedge v_n = \pm |L| e.$$

That is, if we choose coordinates on V that identify V with $\mathbf{R}^n$ so that e is the standard volume form on $\mathbf{R}^n$ then $|L|$ is the absolute value of $\det(v_1, v_2, \ldots, v_n)$. Note that this is in fact invariant under $\mathrm{GL}_n(\mathbf{Z})$ transformations of the basis $v_1, \ldots, v_n$, as it must be since $|L|$ cannot depend on the choice of generators. It's easy to check that the covolume is the only invariant of a lattice in a vector space with a volume form. That is, if V, V' are vector spaces of the same dimension, with volume forms e, e' and lattices L, L', then $|L| = |L'|$ if and only if the exists a linear isomorphism from V to V' that identifies e with e' and takes L to L'.

Note that $|cL| = |c|^n |L|$ for all $c \in \mathbf{R}^*$; thus all lattices in V are equivalent up to scaling. The space of lattices in V with fixed covolume may be identified with the quotient space $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$.

Our next step is to choose an inner-product structure on V that is consistent with the volume form. Two lattices L, L' in inner-product spaces V, V' of the same dimension are equivalent if there is an isometry from V to V' taking L to L'. The space of lattices in V with fixed covolume, up to this equivalence, is then identified with the double quotient space $\mathrm{SO}_n(\mathbf{R})\backslash \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$. For large n, this space is quite complicated, and in general it is believed to be computationally impractical to tell whether two lattices are equivalent in this sense — indeed, some proposed schemes for public-key cryptography depend on this difficulty! [You might search for `lattice cryptography` on the Web.] But for small n the problem is well-understood, and fortunately our main interest is the case $n = 2$, which we shall see is certainly small enough. Even for $n = 2$ the space of lattices in $\mathbf{R}^n$ of fixed covolume is not quite a manifold of the expected dimension $n^2 - 1 - \binom{n}{2} = (n-1)(n+2)/2$, but an "orbifold" of that dimension: a space that locally looks like the quotient of $\mathbf{R}^d$ by a finite group. The reason is that some lattices have automorphisms (other than -1 when $2|n$). The group of automorphisms is always finite, being the intersection of the discrete group $\mathrm{SL}(L)$ with the compact group $\mathrm{SO}_n(\mathbf{R})$; but it need not be trivial.

The reason we want $n = 2$ — besides the fact that it is the first nontrivial case (all lattices in $\mathbf{R}$ are proportional to $\mathbf{Z}$) — is that we're interested in lattices in $\mathbf{C}$. The structure of $\mathbf{C}$ as an oriented inner-product space is entirely captured by the arithmetic of the complex numbers: a linear transformation is an orientation-preserving isometry if and only if it is multiplication by a complex number of absolute value 1. Thus two lattices $L, L' \subset \mathbf{C}$ are equivalent up to scaling if and only if there exists $c \in \mathbf{C}^*$ such that $L' = cL$. We may always choose c such that L is equivalent to a lattice $\mathbf{Z} + \mathbf{Z}\tau$ for some τ in the upper half-plane $\mathcal{H} := \{\tau : \mathrm{Im}(\tau) > 0\}$. Specifically, if $L = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ then $\omega_1 \notin \mathbf{R}\omega_2$, so $\tau := \omega_1/\omega_2$ is either in the upper or the lower half-plane; replacing ω_1 by $-\omega_1$ if necessary, we put τ in $\mathcal{H}$; and then we take $c = \omega_2^{-1}$. The general choice of generators is $(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. [Not $\mathrm{GL}_2(\mathbf{Z})$, since we need determinant $+1$ to preserve the orientation, which also keeps τ in $\mathcal{H}$.] We deduce that for $\tau, \tau' \in \mathcal{H}$ the lattices $\mathbf{Z} + \mathbf{Z}\tau$ and $\mathbf{Z} + \mathbf{Z}\tau'$ are equivalent if and only if $\tau' = (a\tau + b)/(c\tau + d)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$; that is, if τ, τ' are in the same orbit under the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{H}$ by fractional linear transformations. Later we shall study this action further. For now we note that we've identified the space of lattices in $\mathbf{C}$ with the quotient space $\mathcal{H}/\mathrm{SL}_2(\mathbf{Z})$, or equivalently with $\mathcal{H}/\mathrm{PSL}_2(\mathbf{Z})$ since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ acts trivially on $\mathcal{H}$.

Exercises

1. Prove the remaining equivalences among characterizations (i)–(vii) of lattices in a real vector space.

2. Prove the Corollary of Lemma 1.

3. What is the group of isometries of the lattice $\mathbf{Z}^n \subset \mathbf{R}^n$ (with the standard inner product on $\mathbf{R}^n$)?

The next two exercises assume familiarity with the *p-adic integers* $\mathbf{Z}_p$ and the *p-adic numbers* $\mathbf{Q}_p$. If you are comfortable with discrete valuation rings and their fraction fields, you can generalize to that setting.

4. A "lattice" in an n-dimensional vector space W over $\mathbf{Q}_p$ is the image of $\mathbf{Z}_p^n \subset \mathbf{Q}_p^n$ under a bijective linear map from $\mathbf{Q}_p^n$ to W. State equivalent conditions, analogous to (i)–(vii), for such "lattices", and prove their equivalence.

5. Suppose we fix a generator of $\wedge^n(W)$. Define an invariant of a "lattice" in W that plays the role of $|L|$ for a lattice L in a real vector space V. Can you obtain a manifestly intrinsic definition of your invariant, corresponding to the definition of $|L|$ as the volume of V/L?

Doubly periodic functions: preliminaries. Let f be any function on a real vector space V. A *period* of f is a vector $v \in V$ such that $f(x+v) = f(x)$ for all $x \in V$. Clearly these constitute a subgroup of V (in particular zero is always a period). If f is continuous then the periods constitute a closed subgroup $G \subset V$, and f may be regarded as a function on the quotient space V/G, and thus also on V/H for any closed subgroup $H \subset G$. Evidently $G = V$ if and only if f is constant.

Again our main interest is the case $V = \mathbf{C}$. Usually we're concerned only with meromorphic functions f. Unless f is constant, the group of periods of f must be discrete, else for any $z_0 \in \mathbf{C}$ that isn't a pole of f the meromorphic function $f(z) - f(z_0)$ would have infinitely many zeros in each neighborhood of z_0. Hence G must be either $\{0\}$, an infinite cyclic group, or a lattice in $\mathbf{C}$. We say that f is *aperiodic*, *periodic*, or *doubly periodic* accordingly — this last since such a function satisfies two independent periodicity conditions.

Given an additive subgroup $G \subset \mathbf{C}$, consider the meromorphic functions whose group of periods contains G; that is, the meromorphic functions f on $\mathbf{C}$ such that $f(z+g) = f(z)$ for all $z \in \mathbf{C}$ and $g \in G$. These functions clearly constitute a field, call it F. We assume that G is discrete, else we have seen already that F is just the field of constant functions. Then F may be regarded also as the field of meromorphic functions on the Riemann surface $S = \mathbf{C}/G$. For $G = \{0\}$, these are "simply" the meromorphic functions on $\mathbf{C}$. If G is an infinite cyclic group, say $G = \mathbf{Z}\omega$, then we have already identified $S = \mathbf{C}/G$ with $\mathbf{C}^*$ via the exponential map $z \mapsto \exp(2\pi i z/\omega)$. Thus the ω-periodic merormophic functions are "simply" the meromorphic functions on $\mathbf{C}^*$. This leaves only the doubly periodic case, which must look different because here S is compact: it is homeomorphic with the torus $\mathbf{T}^2$. So far we have determined the function field

of only one compact Riemann surface, namely the Riemann sphere $\mathbf{P}^1(\mathbf{C})$; but $\mathbf{T}^2$ cannot be isomorphic with $\mathbf{P}^1(\mathbf{C})$, because $\mathbf{T}^2$, unlike $\mathbf{P}^1(\mathbf{C})$, is not simply connected.

We fix a lattice L, and study the associated field F of doubly-periodic functions. Such a function f may be regarded as:

i) A meromorphic function $f : \mathbf{C} \to \mathbf{P}^1(\mathbf{C})$ such that $f(z+\omega) = f(z)$ for all $z \in \mathbf{C}$ and $\omega \in L$;
ii) A meromorphic function on the complex torus $\mathbf{C}/L$;
iii) A meromorphic function φ on $\mathbf{C}^*$ such that $\varphi(q\zeta) = \varphi(\zeta)$ for all $\zeta \in \mathbf{C}^*$.

This last requires some explanation. Fix generators ω_1, ω_2 of L. The map $\zeta : z \mapsto \exp(2\pi i z/\omega_2)$ is invariant under translation by ω_2. Thus any $f \in F$ is automatically a meromorphic function of ζ. If φ is a meromorphic function on $\mathbf{C}^*$ then the meromorphic function $\varphi \circ \zeta$ on $\mathbf{C}$ is automatically invariant under translation by ω_2, and so is in F if and only if it is invariant also under translation by ω_1. But this is the case if and only if φ is invariant under scaling by

$$q = \exp(2\pi i \omega_1/\omega_2).$$

In terms of our previous notation, this is $q = \exp(2\pi i\tau)$. In particular $0 < |q| < 1$ because $\tau \in \mathcal{H}$. Equivalently, our torus is also isomorphic with the Riemann surface $\mathbf{C}^*/q^{\mathbf{Z}}$. Note that in general different choices of ω_1, ω_2 will yield different values of q, all producing isomorphic Riemann surfaces $\mathbf{C}^*/q^{\mathbf{Z}}$; in fact τ, τ' yield the same q if and only if τ, τ' are in the same orbit of the infinite cyclic subgroup of $\mathrm{SL}_2(\mathbf{Z})$ generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

The reason we're concerned with the field F, rather than the ring of doubly-periodic holomorphic functions, is (as was the case for $\mathbf{P}^1(\mathbf{C})$, and for much the same reason) that the holomorphic functions in F give us nothing new:

Lemma 2. *A doubly-periodic holomorphic function is constant.*

Proof: Suppose f is such a function. Since $|f(\cdot)|$ is a continuous function on the compact space $\mathbf{C}/L$, it must attain its supremum on that space. But then f must be constant by the maximum principle. □

Note that this used formulation (ii) of double periodicity. We could also have used formulation (i). Fix generators ω_1, ω_2 as before, and let $P \subset \mathbf{C}$ be the *period parallelogram*

$$P := \{a_1\omega_1 + a_2\omega_2 : a_1, a_2 \in [0, 1)\}.$$

This is a fundamental region for the action of L on $\mathbf{C}$ by translation: every $z \in \mathbf{C}$ is uniquely $z_0 + \omega$ for some $z_0 \in P$ and $\omega \in L$. Hence $f(z) \subseteq f(P) \subseteq f(\overline{P})$. But $\overline{P}$ is compact, so $f(\overline{P})$ is bounded. Therefore $f(\mathbf{C})$ is bounded, whence f is constant by Liouville's theorem.

Corollary. *The only holomorphic differentials on $\mathbf{C}/L$ are $c\,dz$ for $c \in \mathbf{C}$.*

Proof: The differential $f(z)\,dz$ is holomorphic if and only if f is. □

If $f \in F$ is nonconstant then it has at most finitely many zeros or poles in $\mathbf{C}/L$, because the zeros constitute a discrete set in a compact space. We shall see that in fact the numbers of zeros and poles, counted with multiplicity, are equal. By applying this result to the meromorphic function $f - c$, we'll deduce that the same is true also of the number of times f takes on the value c for each $c \in \mathbf{C}$. That is, there exists a positive integer, which we shall call the *degree* of f and denote by $\deg(f)$, such that all points in $\mathbf{P}^1(\mathbf{C})$ have $\deg(f)$ preimages under f, counted with multiplicity. This in fact holds for meromorphic functions on any compact Riemann surface. We have already seen the case of meromorphic functions on $\mathbf{P}^1(\mathbf{C})$. The general result can be proved in several ways; we shall obtain it as a corollary of another result concerning differentials.

Lemma 3. *The sum of the residues of any meromorphic differential on $\mathbf{C}/L$ vanishes.*

The classical statement of this result in terms of doubly periodic functions is: *the residues in a period parallelogram of any doubly periodic function sum to zero.*

Proof: The general meromorphic differential is $f(z)\,dz$ for some $f \in F$. Choose $z_0 \in \mathbf{C}$ such that the boundary of the translate $P' = z_0 + P$ of the period parallelogram does not pass through any pole of f. The sum of the residues is then $(2\pi i)^{-1} \oint_{\partial P'} f(z)\,dz$. But the integral vanishes because on each pair of parallel sides of P' the integrands are equal and are integrated in opposite directions. □

Much the same proof applies to meromorphic differentials ϕ on any compact Riemann surface S. The following Corollary generalizes likewise. One formulation of the proof is to triangulate S, making sure the sides of the triangles do not go through any poles of ϕ. Then the sum of the residues of ϕ is the sum of $(2\pi i)^{-1} \oint_{\partial T} \phi$ as T ranges over the triangles; but each side of a triangle occurs twice in the sum, and the integrals on it cancel. Another way to say this is to remove from S small circles about the poles of ω, leaving a Riemann surface with boundary S_1, and consider $(2\pi i)^{-1} \oint_{\partial S_1} \omega$. On the one hand this vanishes by the appropriate version of the Cauchy integral theorem; but on the other hand each pole of ω contributes its residue to the integral. So the sum of the residues equals zero as claimed.

Corollary. *Let f be any meromorphic function on $\mathbf{C}/L$ other than the constant function zero. Then f has as many zeros as poles in $\mathbf{C}/L$, counted with multiplicity.*

The classical statement of this result in terms of doubly periodic functions is: *a doubly periodic function that is not identically zero has as many zeros as poles, counted with multiplicity, in a period parallelogram.*

Proof: Apply Lemma 3 to the "logarithmic differential" df/f.

As noted already, it follows that the preimage under a nonconstant function

$f \in F$ of any $c \in \mathbf{P}^1(\mathbf{C})$, consists of the same number of points, counted with multiplicity. This number is called the degree of f; by convention (which agrees with the usual convention for rational functions), a constant function is deemed to have degree zero.

There is an additional and subtler condition that the zeros of a doubly-periodic function must satisfy:

Proposition 1. *Let f be any meromorphic function on $\mathbf{C}/L$ other than the constant function zero. Then the sum of the zeros of f, counted with multiplicity, equals the sum of the poles of f, counted with multiplicity.*

That is to say, if the zeros (poles) of f, listed with multiplicity, are z_j (z'_j) for $1 \leq j \leq \deg(f)$, then

$$\sum_{j=1}^{\deg(f)} z_j = \sum_{j=1}^{\deg(f)} z'_j.$$

Note that the sum is taking place in $\mathbf{C}/L$. If we regard f as a doubly periodic function on $\mathbf{C}$, we must lift the z_j and z'_j from $\mathbf{C}/L$ to representatives $\tilde{z}_j, \tilde{z}'_j \in \mathbf{C}$, for instance by requiring that they lie in a period parallelogram; then Proposition 1 asserts that

$$\sum_{j=1}^{\deg(f)} \tilde{z}_j - \sum_{j=1}^{\deg(f)} \tilde{z}'_j \in L.$$

Note that our formulations of this identity implicitly use Corollary 3. In fact that Corollary follows from Proposition 1. To see this, apply this Proposition to $f(z-c)$ for any $c \in \mathbf{C}/L$. The zeros and poles of this function are the same as those of f, shifted by c. For the sums to be equal for any c, there must be as many zeros as poles.

Proof of Prop.1: As before, choose $z_0 \in \mathbf{C}$ such that the boundary of the translate $P' = z_0 + P$ of the period parallelogram does not pass through any pole of f. Let $\tilde{z}_j, \tilde{z}'_j$ be the zeros and poles of f in P'. Then

$$\sum_j (\tilde{z}_j - \tilde{z}'_j) = \frac{1}{2\pi i} \oint_{\partial P'} z \frac{f'(z)}{f(z)}\, dz.$$

We write

$$\oint_{\partial P'} = \left(\int_{z_0+\omega_2}^{z_0+\omega_1+\omega_2} - \int_{z_0}^{z_0+\omega_1} \right) + \left(\int_{z_0}^{z_0+\omega_2} - \int_{z_0+\omega_2}^{z_0+\omega_1+\omega_2} \right).$$

On each pair of edges of P', the functions f'/f agree, while z changes by ω_2 or ω_1. Subtracting, we find

$$\oint_{\partial P'} z \frac{f'(z)}{f(z)}\, dz = \omega_2 \int_{z_0}^{z_0+\omega_1} \frac{f'(z)}{f(z)}\, dz + \omega_1 \int_{z_0+\omega_2}^{z_0} \frac{f'(z)}{f(z)}\, dz$$

Each of the two integrals on the right-hand side is an integral multiple of $2\pi i$, because $f'/f = (\log f)'$ and $f(z_0) = f(z_0 + \omega_1) = f(z_0 + \omega_2)$. Hence the sum of the integrals is in $2\pi i L$, whence $(2\pi i)^{-1} \oint_{\partial P'} z(f'(z)/f(z))\, dz \in L$. □

We shall see that conversely if $\sum_{j=1}^{\deg(f)} z_j = \sum_{j=1}^{\deg(f)} z'_j$ then there exists $f \in F$ whose zeros and poles are at z_j and z'_j respectively. Proposition 1, and this converse, also generalize to meromorphic functions on an arbitrary Riemann surface S of genus g, where one finds g conditions on the zeros and poles rather than the single condition of Proposition 1. But it takes considerably more work to state, let alone prove, these generalizations — except in the case $S = \mathbf{P}^1(\mathbf{C})$, when $g = 0$ (so there is no condition beyond the equality of the numbers of zeros and poles) and the existence of a rational function with prescribed zeros and poles is well-known and elementary.

We conclude this section with an important consequence of Prop. 1:

Corollary. *There is no doubly-periodic function of degree* 1.

Proof: such a function would have a single zero z_1, and a single pole z'_1. But then $z_1 \neq z'_1$ (a point of $\mathbf{C}/L$ cannot be both zero and pole), contradicting Proposition 1. □

This result could also be proved topologically: a function of degree 1 on $\mathbf{C}/L$ would be a homeomorphism from $\mathbf{C}/L$ to $\mathbf{P}^1(\mathbf{C})$, which is impossible because $\mathbf{P}^1(\mathbf{C})$ is simply connected but $\mathbf{C}/L$ is not.

Exercises

The next three exercises are stated for doubly periodic functions, but hold (with the same proof) for meromorphic functions on any compact Riemann surface; in particular they hold for pairs of rational functions.

1. ("triangle inequality" for degrees) Show that $\deg(f + g) \leq \deg(f) + \deg(g)$ for all $f, g \in F$. When does equality hold? Can you use the degree to construct a nontrivial metric space from F?

2. Prove that any $f, g \in F$ are algebraically dependent. [Use linear algebra to show that for d, e large enough there exists a linear combination among the monomials $f^j g^k$ ($j \leq d$, $k \leq e$) that has no poles, and is thus constant. How large must d, e be in terms of $\deg(f)$ and $\deg(g)$?]

3. Prove that if $f \in F$ is nonconstant then $F/\mathbf{C}(f)$ is a field extension of finite degree, which is a factor of $\deg(f)$. [Suppose $F \supseteq F' \supseteq \mathbf{C}(f)$ and $[F' : \mathbf{C}(f)] = d < \infty$. We know from field algebra that any field extension of finite degree is generated by one element. Thus $F' = \mathbf{C}(f, g)$ for some $g \in F$ satisfying a polynomial equation $P(f, g) = 0$ of degree d in g. This yields a map from $\mathbf{C}/L$ to the Riemann surface of $P(z, w) = 0$; what is the degree of this map?]

It is known that in fact $[F' : \mathbf{C}(f)] = \deg(f)$, and that this too generalizes to arbitrary compact Riemann surfaces. You should be able to verify it directly for $\mathbf{P}^1(\mathbf{C})$.

Doubly periodic functions: the Weierstrass approach.

There are several ways to construct and study doubly-periodic functions. We shall give two approaches that correspond to our two expansions of a general meromorphic function on $\mathbf{C}$: the "additive" approach, using sums of partial fractions to account for the principal parts at the poles, and the "multiplicative" approach, using products to account for the zeros and poles. We begin with the additive approach, due to Weierstrass.

Fix a lattice $L \in \mathbf{C}$, and let F be its field of doubly periodic functions. By the Corollary to Proposition 1, a nonconstant function in F must have at least two poles in each period parallelogram. We construct such a function, the *Weierstrass $\wp$-function* $\wp \in F$, with a double pole at each lattice point and no other poles. By Lemma 3, the residues of $\wp\, dz$ at these poles must vanish. Hence there exists $a \in \mathbf{C}^*$ such that the principal part of f at each double pole $c \in L$ is $a(z-\omega)^{-2}$. Our $\wp$ will have $a = 1$.

We shall use $\sum'_{\omega\in L}$ to mean the sum over all nonzero $\omega \in L$. For instance, the Corollary to Lemma 1, applied to L, states that $\sum'_{\omega\in L} |\omega|^{-s}$ converges if and only if $s > 2$. Thus $\sum_{\omega\in L}(z-\omega)^{-2}$, which would be our first attempt at constructing $\wp(z)$, does not converge absolutely for any $z \in \mathbf{C}$, but

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega\in L}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

does converge uniformly in compact subsets of $\mathbf{C}-L$, because on any such subset $(z-\omega)^{-2} - \omega^{-2} = O(|\omega|^{-3})$. Hence $\wp(z)$ is an analytic function on $\mathbf{C}-L$, with double poles of the desired principal parts at lattice points. Moreover, the sum defining $\wp(z)$ can be differentiated termwise to obtain

$$\wp'(z) := -2 \sum_{\omega\in L} \frac{1}{(z-\omega)^3},$$

the sum again converging uniformly in compact subsets of $\mathbf{C} - L$. It is evident that this function $\wp'$ is doubly periodic of degree 3, and is odd: $\wp'(-z) = -\wp'(z)$ for all $z \in \mathbf{C} - L$. With some more work we establish the corresponding result for $\wp$:

Proposition 2. *The function $\wp$ is an even, doubly periodic function of degree* 2.

Proof: That $\wp(z) = \wp(-z)$ is clear from the sum defining $\wp$. We noted already that $\wp$ has double poles at each $\omega \in L$ and no other poles. It thus remains to show that $\wp(z+\omega) = \wp(z)$ for all $\omega \in L$ and $z \in \mathbf{C} - L$. The difference $\wp(z+\omega) - \wp(z)$ is a constant function, because its derivative is $\wp'(z+\omega) - \wp'(z)$, which vanishes because $\wp' \in F$. In particular,

$$\wp(z+\omega) - \wp(z) = \wp(-(z+\omega)+\omega) - \wp(-(z+\omega)) = -\big(\wp(-(z+\omega)) - \wp(-z)\big).$$

But also $\wp(z+\omega) - \wp(z) = \wp(-(z+\omega)) - \wp(-z)$ because $\wp$ is even. Hence $\wp(z+\omega) - \wp(z) = 0$ as claimed. □

Alternatively we could have used $\wp(\omega_1/2) = \wp(-\omega_1/2)$ and $\wp(\omega_2/2) = \wp(-\omega_2/2)$ for generators ω_1, ω_2 of L.

Corollary. *For $z, z' \in \mathbf{C} - L$ we have $\wp(z) = \wp(z')$ if and only if $z - z' \in L$ or $z + z' \in L$. If $z_0 \in \frac{1}{2}L - L$ then z_0 is a double zero of $\wp(z) - \wp(z_0)$.*

(Thus $\wp$ is an explicit isomorphism from the Riemann surface $(\mathbf{C}/L)/\{\pm 1\}$ to $\mathbf{P}^1(\mathbf{C})$.)

Proof: For any $z' \in \mathbf{C} - L$ we have the function $\wp - \wp(z') \in F$ of degree 2. This function vanishes when $z - z' \in L$, by double periodicity, and when $z + z' \in L$, because $\wp$ is also even. We have thus accounted for both zeros of $\wp - \wp(z')$ in $\mathbf{C}/L$, provided $2z' \notin L$. If $2z' \notin L$ then $\wp(z - z')$ is an even function of z, because $\wp(-z - z') = \wp(z + z') = \wp(z + z' - 2z) = \wp(z - z')$. Hence in this case $\wp - \wp(z')$ has a double zero at z', and we have again accounted for all the zeros of $\wp - \wp(z')$ in $\mathbf{C}/L$. □

In particular the zeros of $\wp$ in are $w, -w$ for some $w \in \mathbf{C}/L$. In general there is no nice description of $\pm w$ in terms of L. On the other hand, the zeros of $\wp'$ are readily located: If $z' \in \frac{1}{2}L - L$ then $\wp'(z - z')$ is an odd function of z, since it is the derivative of an even function; in particular, $\wp'(-z') = 0$. [We had to require $z' \notin L$, else $-z'$ would be a pole of $\wp'$ rather than a zero.] Since $(\frac{1}{2}L - L)/L$ has cardinality 3, which equals the degree of $\wp'$, we have thus accounted for all the zeros of $\wp'$: they are precisely the half-lattice points.

We next show that $\wp$ and $\wp'$ generate all the doubly periodic functions. Let $A \subset F$ be the ring of doubly periodic functions with no poles except possibly at lattice points. We have seen that $\wp, \wp' \in A$. In fact we prove:

Proposition 3. *i) We have $A = \mathbf{C}[\wp, \wp']$. That is, $f \in A$ if and only if f can be written a polynomial in $\wp, \wp'$ with complex coefficients.*
ii) The fraction field of A is F. That is, $F = \mathbf{C}(\wp, \wp')$. Therefore F consists of all functions f_1/f_2 where $f_1, f_2 \in \mathbf{C}[\wp, \wp']$ and f_2 is not the zero function.

Proof: i) Use induction on $d = \deg(f)$. If $d = 0$ then f is the constant function; else $d > 1$ by the Corollary to Proposition 1. Let c be the leading coefficient in the Laurent expansion of f about $z = 0$, so $f(z) = cz^{-d} + O(z^{1-d})$ for small $z \neq 0$. We find $f_1 \in \mathbf{C}[\wp, \wp']$ of degree d with the same leading coefficient. Then $f - f_1 \in A$ has degree $< d$, so by the inductive assumption $f - f_1 \in \mathbf{C}[\wp, \wp']$, whence $f \in \mathbf{C}[\wp, \wp']$. Specifically, we take for f_1 the following monomial: if d is even then $f_1 = c\,\wp^{d/2}$; if d is odd then $f_1 = -c\,\wp^{(d-3)/2}\wp'/2$ (it is here that we use $d > 1$). This completes the induction step and proves part (i).

ii) Let $f \in F$. If f is the zero function we are done. Else let z_j be the nonzero poles of f in $\mathbf{C}/L$, and let m_j be the multiplicity of the pole at z_j. Set $f_2 = \prod_j (\wp - \wp(z_j))^{m_j} \in \mathbf{C}[\wp] \subset A$. Then $f_1 := f_2 f \in A$, and we have written f as the quotient f_1/f_2 with $f_1, f_2 \in A$ as desired. □

This does not yet determine the structure of A and F, because $\wp, \wp'$ must be algebrically dependent (see the previous set of Exercises). We next determine this relation and identify A and F.

First we make the statement of Propostion 3 more precise. Let $A_+ \subset A$ and $F_+ \subset F$ be the subring and subfield of even doubly-periodic functions, that is, functions satisfying the identity $f(z) = f(-z)$. Let $A_- \subset A$ and $F_- \subset F$ be the odd functions, which constitute respectively an A_+-module and an F_+-vector space. Note that $A = A_+ \oplus A_-$ and $F = F_+ \oplus F_-$, thanks to the identity

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}$$

expressing an arbitrary $f \in F$ uniquely as the sum of an even and an odd function, both of which are in A if f is.

Lemma 4. *$A_+ = \mathbf{C}[\wp]$, $A_- = \wp'\mathbf{C}[\wp]$, $F_+ = \mathbf{C}(\wp)$, and $F_- = \wp'\mathbf{C}(\wp)$.*

Proof: Our proof of Proposition 3 yields an expression for any $f \in A$ as $P(\wp) + \wp' Q(\wp)$ for some polynomials $P, Q \in \mathbf{C}[X]$, and for any $f \in F$ as $r(\wp) + \wp' s(\wp)$ for some rational functions $r, s \in \mathbf{C}(X)$. Lemma 4 then follows from the observation that $P(\wp)$ and $r(\wp)$ are always even and $\wp' Q(\wp)$ and $\wp' s(\wp)$ are always odd. □

In particular, $\wp'^2$ is an even function, regular except for sextuple poles at lattice points. Hence $\wp'^2 \in A_+$, so $\wp'^2$ is a polynomial in $\wp$, necessarily of degree 3. Comparing leading coefficients, we see that this polynomial has leading coefficient 4.

To determine the remaining coefficients of this cubic, we compare Laurent expansions at the origin. Each term $(z - \omega)^{-2} - \omega^{-2}$ in the sum defining $\wp$ has the elementary Taylor expansion

$$\sum_{n=1}^{\infty} (n+1)\omega^{-(n+2)} z^n = \frac{2z}{\omega^3} + \frac{3z^2}{\omega^4} + \frac{4z^3}{\omega^5} + \frac{5z^4}{\omega^6} + \cdots$$

about $z = 0$. Summing over nonzero $\omega \in L$, we find

$$\wp = \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1)\gamma_{n+2} z^n,$$

where for integers $k > 2$ we define $\gamma_k = \gamma_k(L)$ to be the absolutely convergent sum

$$\gamma_k := \sum_{\omega \in L}{}' \omega^{-k}.$$

By matching ω with $-\omega$ (or recalling that $\wp$ is even) we see that $\gamma_k = 0$ for all odd k. [Hence the alternative indexing of these sums, as in Ahlfors, where G_k is used for what we call γ_{2k}.] We are left with

$$\wp = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)\gamma_{2k+2} z^{2k} = \frac{1}{z^2} + 3\gamma_4 z^2 + 5\gamma_6 z^4 + 7\gamma_8 z^6 + \cdots,$$

$$\wp' = -\frac{2}{z^3} + \sum_{k=1}^{\infty} 2k(2k+1)\gamma_{2k+2} z^{2k-1} = -\frac{2}{z^3} + 6\gamma_4 z + 20\gamma_6 z^3 + 42\gamma_8 z^5 + \cdots.$$

Hence

$$\wp'^2 - 4\wp^3 = -60\gamma_4 z^{-2} - 140\gamma_6 - (72\gamma_4 + 252\gamma_8)z^2 - (120\gamma_4\gamma_6 + 396\gamma_{10})z^4 \cdots$$

and

$$\wp'^2 - 4\wp^3 + 60\gamma_4\wp + 140\gamma_6 = (108\gamma_4^2 - 252\gamma_8)z^2 + (180\gamma_4\gamma_6 - 396\gamma_{10})z^4 \cdots$$

Hence $\wp'^2 - 4\wp^3 + 60\gamma_4\wp + 140\gamma_6$ is a doubly periodic function with no poles, and indeed with a zero at $z = 0$. Therefore it is the zero function, and we have proved the *Weierstrass differential equation*

$$\wp'^2 = 4\wp^3 - 60\gamma_4\wp - 140\gamma_6.$$

It also follows that the Taylor coefficients $108\gamma_4^2 - 252\gamma_8$, $180\gamma_4\gamma_6 - 396\gamma_{10}$, etc. of $\wp'^2 - 4\wp^3 + 60\gamma_4\wp + 140\gamma_6$ must vanish. This yields a sequence of remarkable identities

$$\gamma_8 = \frac{3}{7}\,\gamma_4^2, \quad \gamma_{10} = \frac{5}{11}\,\gamma_4\gamma_6, \ldots$$

that hold for every lattice L. An easy recursion for these identities can be obtained by differenting the Weierstrass formula for $\wp'^2$ and dividing by $2\wp$. This yields the differential equation

$$\wp'' = 6\wp^2 - 30\gamma_4.$$

Now for $k = 1, 2, 3, \ldots$ the z^{2k} coefficient of $\wp''$ is $(2k+1)(2k+2)(2k+3)\gamma_{2k+4}$, while the z^{2k} coefficient of $6\wp^2 - 30\gamma_4$ is

$$12(2k+3)\gamma_{2k+4} + 6\sum_{j=1}^{k-1}(2j+1)(2(k-j)+1)\gamma_{2(j+1)}\gamma_{2(k-j+1)}.$$

Equating these yields a formula for $2(k-1)(2k+3)(2k+5)\gamma_{2k+4}$ as a polynomial in $\gamma_4, \gamma_6, \ldots, \gamma_{2k}$. Once $k > 1$ we can solve for γ_{2k+4}, and recursively obtain each of $\gamma_8, \gamma_{10}, \gamma_{12}, \ldots$ as polynomials in γ_4 and γ_6 with rational coefficients.

We return now to more structural consequences of the Weierstrass equation. Let $P_L(X)$ be the cubic polynomial $4X^3 - 60\gamma_4 X - 140\gamma_6$. The identity $\wp'^2 = P_L(\wp)$ yields a homomorphism from A to the quotient ring $\mathbf{C}[X,Y]/(Y^2 - P_L(X))$ in which $\wp, \wp'$ are mapped to X, Y. We readily see that this map is in fact an isomorphism; that is, if $Q \in \mathbf{C}[X,Y]$ is any polynomial such that $Q(\wp, \wp')$ is the zero function then Q is a multiple of $Y^2 - P_L(X)$. Indeed, every $Q \in \mathbf{C}[X,Y]$ is congruent modulo $Y^2 - P_L(X)$ with a polynomial of degree at most 1 in Y, say $A(X) + YB(X)$ for some $A, B \in \mathbf{C}[X]$. If $Q(\wp, \wp') = 0$ then also $A(\wp) + \wp' B(\wp) = 0$. Separating this identity into its even and odd parts we find that $A(\wp) = B(\wp) = 0$, whence A and B are identically zero and Q is a multiple of $Y^2 - P_L(X)$ as claimed.

In algebraic geometry, $\mathbf{C}[X,Y]/(Y^2 - P_L(X))$ is the ring of regular functions on the affine curve $Y^2 = P_L(X)$, and the quotient field of this ring is the function

field of the corresponding projective curve. It quickly follows from the Corollary to Proposition 2 that $z \mapsto (\wp(z), \wp'(z))$ is a bijection from $(\mathbf{C} - L)/L$ to the solutions $(x, y) \in \mathbf{C}^2$ of $y^2 = P_L(x)$. Indeed for any such solution the function $\wp - x \in A$ has two zeros $z, -z$ in $(\mathbf{C} - L)/L$, and since $\wp'(-z) = -\wp'(z)$ the values of $\wp'$ at these solutions of $\wp = x$ are the two square roots of $P_L(x)$, unless $z \equiv -z \bmod L$ in which case $\wp'(z) = 0$.

It takes only a bit more effort to check that $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism from $(\mathbf{C} - L)/L$ to the affine Riemann surface of $y^2 = P_L(x)$, which extends to an isomorphism from $\mathbf{C}/L$ to the corresponding projective Riemann surface (obtained by adding the point at infinity $x = y = \infty$). In general, the construction of the Riemann surface of a polynomial equation such as $y^2 = P_L(x)$ may require resolving a few singular points, but here the locus of $y^2 = P_L(x)$ is already smooth; equivalently, P_L has only simple roots. We can see this by locating the roots. We found already that the zeros of $\wp'$ are the three half-lattice points. We now recognize these zeros also as the double zeros of $P_L(\wp)$; hence the values of $\wp$ at these half-lattice points are *simple* zeros of P_L. That they are distinct is again a special case of the Corollary to Proposition 2.

In summary, we have:

Theorem 1. *i) The map $(\wp, \wp') \mapsto (X, Y)$ is an isomorphism from A and $\mathbf{C}[X, Y]/(Y^2 - P_L(X))$.*
ii) The map $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism from $\mathbf{C}/L$ to the projective Riemann surface of $Y^2 = P_L(X)$. In particular, every solution $(x, y) \in \mathbf{C}^2$ of $y^2 = P_L(x)$ arises as $(\wp(z), \wp'(z))$ for some $z \in \mathbf{C} - L$, determined uniquely up to translation by L.
iii) The polynomial P_L has no repeated roots.

We shall see that (iii) is the only condition on P_L when we vary L — that is, that for every $a, b \in \mathbf{C}$ such that the cubic $4X^3 + aX + b$ has distinct roots (equivalently: such that $a^3 + 27b^2 \neq 0$), there exists a lattice L for which $P_L(X) = 4X^3 + aX + b$; and moreover, such that this lattice is uniquely determined by P. In other words, $20\gamma_4^3 \neq 49\gamma_6^2$ is the only conditions on γ_4, γ_6, and any complex numbers satisfying this condition arise for a unique lattice L.

We next prove, as promised, that Proposition 1 is the only condition on the zeros and poles of a doubly-periodic function. It will be convenient to introduce the following terminology from the language of algebraic geometry:

Definitions. *i) A* divisor *on a Riemann surface S is a finite formal linear combination $D = \sum_{n=1}^{d} a_n (z_n)$ of points $z_n \in S$ with integer coefficients a_n. The* degree *of D, denoted* $\deg(D)$*, is $\sum_{n=1}^{d} a_n$, the sum of the coefficients. We say $D \geq 0$ if D is a nonnegative linear combination (each $a_n \geq 0$), and $D > 0$ if $D \geq 0$ and $D \neq 0$. For divisors D, E the notations $D \geq E$ and $D > E$ are synonymous with $D - E \geq 0$ and $D - E > 0$ respectively.*
ii) The divisor of zeros $(f)_0$ *of a meromorphic function f on S that has only finitely many zeros in S is $\sum_n a_n (z_n)$, where z_n ranges over the zeros of f and a_n is the multiplicity of the zero at z_n. More generally, for $c \in \mathbf{C}$ we define*

$(f)_c = (f-c)_0$.
iii) The divisor of poles $(f)_\infty$ *of* f *is* $(1/f)_0$.
iv) The divisor (f) *of* f *is* $(f)_0 - (f)_\infty$.
v) For any divisor D *we define a set* $\Gamma(D)$ *of meromorphic functions, consisting of the zero function and all nonzero meromorphic* f *such that* $(f) + D \geq 0$.

The following properties are immediate consequences (exercises):

1. Let D, E, F be any divisors on S. If $D \geq E$ then $\deg(D) \geq \deg(E)$, with equality if and only if $D = E$. if $D \geq E$ and $E \geq F$ then $D \geq F$, with equality if and only if $D = E = F$. Finally, $D > E$ if and only if $D + F > E + F$, and $D \geq E$ if and only if $D + F \geq E + F$.

2. If f, g are holomorphic functions with finitely many zeros then $(fg)_0 = (f)_0 + (g)_0$. If f, g are meromorphic functions with finitely many zeros and poles then $(fg) = (f) + (g)$.

3. $\Gamma(D)$ is a $\mathbf{C}$-vector space for any divisor D.

4. The Corollary to Lemma 3 is equivalent to: $\deg((f)) = 0$ for all meromorphic functions that are not identically zero. Equivalently, $\deg((f)_0) = \deg((f)_\infty)$, and also $\deg((f)_0) = \deg((f)_c)$ if f is not the constant function c.

5. The degree of any nonconstant meromorphic function f on a compact Riemann surface S equals $deg((f)_c)$ for any $c \in \mathbf{P}^1(\mathbf{C})$ unless f is the constant function c.

6. Let $\mathcal{D}$ be the group of divisors on $\mathbf{C}/L$, and $\mathcal{D}_0$ the subgroup of divisors of degree 0. Let σ be the homomorphism from $\mathcal{D}$ to the group $\mathbf{C}/L$ defined by $\sum_n a_n (z_n) \mapsto \sum_n a_n z_n$. We just saw in effect (#2 above) that $f \mapsto (f)$ is a homomorphism from F^* to $\mathcal{D}$, and more precisely (#4 above) that the image of this homomorphism is contained in $\mathcal{D}_0$. The assertion of Proposition 1 is equivalent to the assertion that the composite map $F^* \to \mathbf{C}/L$ is zero.

We are about to prove that in fact the sequence $F^* \to \mathcal{D}_0 \xrightarrow{\sigma} \mathbf{C}/L$ is exact. A divisor of the form (f) is said to be *principal*; the principal divisors constitute a subgroup of $\mathcal{D}$ by #2, and of $\mathcal{D}_0$ by #4. We've seen (Proposition 1) that this subgroup is contained in the kernel of σ, and our goal is to prove that the principal divisors constitute precisely that kernel.

Lemma 5. *If* D *and* E *are divisors on a Riemann surface such that* $D \geq E$ *then* $\Gamma(E)$ *is a subspace of* $\Gamma(D)$*, with codimension at most* $\deg(D - E)$.

Proof: By induction on $\deg(D-E)$ it suffices to prove this when $\deg(D-E) = 1$ (the case $\deg(D-E) = 0$ is trivial). That $\Gamma(E) \subseteq \Gamma(D)$ is clear. Let $D-E = (z)$, and let a be the coefficient of (z) in D. If $f \in \Gamma(D)$ then $v_z(f) \geq -a$, and then $f \in E$ if and only if $v_z(f) > -a$. Hence $\Gamma(E)$ is the kernel of a linear functional on $\Gamma(D)$, and therefore has codimension at most 1 in $\Gamma(D)$. □

The next Lemma is specific to functions on $\mathbf{C}/L$:

Lemma 6. *For all integers* $m > 0$ *the dimension of* $\Gamma(m(0))$ *is* m.

Proof: The space $\Gamma(m(0))$ consists of those $f \in A$ with $v_0(f) \geq -m$ (equiva-

lently, of $f \in A$ of degree at most m). A basis of this space is the disjoint union of $\{\wp^j | 0 \le 2j \le m\}$ with $\{\wp^j \wp' | 0 \le 2j \le m-3\}$. This union is readily seen to have cardinality m whether m is even or odd. □

Proposition 4. *Suppose D is a divisor on $\mathbf{C}/L$ such that $D \ge 0$ and $\sigma(D) = 0$. Then $D - \deg(D) \cdot (0)$ is principal.*

Proof: Let $m = \deg D$. We are claiming the existence of $f \in A$ such that $(f) = D - m\,(0)$. We may assume $m > 0$, because if $m = 0$ then $D = 0$, whence D is the divisor of the constant function 1.

Once $m > 0$ there exists $z \in \mathbf{C}/L$ such that $D - (z) \ge 0$. Since $\deg(D-(z)) < m = \deg(m\,(0))$, the codimension of $\Gamma(m\,(0) - D + (z))$ in $\Gamma(m\,(0))$ is strictly less than m, so $\Gamma(m\,(0) - D + (z))$ has positive dimension by Lemma 6. Let f be a nonzero function in $\Gamma(m\,(0) - D + (z))$. Then $(f) = D - m\,(0) - (z) + E$ for some divisor $E \ge 0$. But $\deg(f) = 0$, so $\deg(E) = 1$, that is, $E = (w)$ for some $w \in \mathbf{C}/L$. Since $\sigma((f)) = \sigma(D) = \sigma(m\,(0)) = 0$, we must have $z = w$. Therefore $(f) = D - m\,(0)$, so $D - m\,(0)$ is principal as claimed. □

We have thus proved that a degree-zero divisor $\sum_n a_n\,(z_n)$ in the kernel of σ is principal, but only under the assumption that $a_n \ge 0$ unless $z_n = 0$. To remove this assumption, we need only note that the differences between pairs of such divisors yield all of $\ker(\sigma : \mathcal{D}_0 \to \mathbf{C}/L)$. Indeed if D is any degree-zero divisor with $\sigma(D) = 0$, write $D = D_1 - D_2$ with $D_j \ge 0$, and let $m = \deg(D_1) = \deg(D_2)$ and $z = \sigma(D_1) = \sigma(D_2)$. Then the degree-zero divisors

$$E_j := D_j + (-z) - (m+1)\,(0)$$

are in $\ker(\sigma)$, and are therefore principal by Proposition 4; say $E_j = (f_j)$. Since $D = E_1 - E_2$, we deduce that D is the principal divisor (f_1/f_2). We have thus proved:

Theorem 2. *A divisor D on $\mathbf{C}/L$ is principal if and only if $\deg(D) = 0$ and $\sigma(D) = 0$.*

One consequence is the *addition formula* for $\wp$, which expresses $\wp(z_1 + z_2)$ as a rational function of $\wp(z_1)$, $\wp'(z_1)$, $\wp(z_2)$, and $\wp'(z_2)$. By differentiating with respect to either z_1 or z_2 we obtain also the formula for $\wp'(z_1 + z_2)$.

Choose $z_3 \in \mathbf{C}/L$ such that $z_1 + z_2 + z_3 = 0$. Assume that the z_j are distinct and nonzero. Then $(z_1) + (z_2) + (z_3) - 3(0)$ is a degree-zero divisor in the kernel of σ, so by Theorem 2 (or even by Proposition 4) it is the divisor of some $f \in F$, indeed of some $f \in A$ because f is regular apart from the triple pole at 0. Thus f is a scalar multiple of $\wp' - \alpha\wp - \beta$ for some constants α, β, which can be calculated by solving $f(z_1) = f(z_2) = 0$ as simultaneous linear equations in α, β. (These equations are independent because $(\wp(z_1), \wp'(z_1)) \ne (\wp(z_2), \wp'(z_2))$ by Theorem 1ii.) But then $\wp'(z_3) = \alpha\wp(z_3) + \beta$. This, together with the identity ${\wp'}^2 = P_L(\wp)$, means that $\wp(z_3)$ is a root of the cubic $P_L(X) - (\alpha X + \beta)^2 = R(X)$, say. By the same argument, $\wp(z_1)$ and $\wp(z_2)$ are roots of this cubic, and the $\wp(z_j)$ are distinct by our hypotheses on the z_j. In particular, since R has leading

coefficient 4 and its X^2 coefficient is $-\alpha^2$ we have

$$\wp(z_1) + \wp(z_2) + \wp(z_3) = \frac{\alpha^2}{4} = \left(\frac{1}{2} \frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)} \right)^2 .$$

We have thus written $\wp(z_3)$, and hence also $\wp(z_1 + z_2) = \wp(-z_3) = \wp(z_3)$, as a rational function in $\wp(z_1)$, $\wp'(z_1)$, $\wp(z_2)$, and $\wp'(z_2)$, as promised. If some of the z_j coincide with each other, or with zero, we can still obtain $\wp(z_1 + z_2)$ by taking a suitable limit in this formula; for instance,

$$\wp(2z) = \left(\frac{\wp''(z)}{2\wp'(z)} \right)^2 - 2\wp(z),$$

and we already saw that $\wp'' = 6\wp^2 - 30\gamma_4$.

The fact that $z_1 + z_2 + z_3 = 0$ if and only if there exist scalars α, β such that $\wp'(z_j) = \alpha\wp(z_j) + \beta$ for $j = 1, 2, 3$ has a beautiful geometrical interpretation: $z_1 + z_2 + z_3 = 0$ if and only if the points $(\wp(z_j), \wp'(z_j))$ on the elliptic curve $Y^2 = P_L(X)$ are collinear. If $z_1 = z_2 = z \neq z_3$ then z_3 is the curve's third point of intersection with the tangent to the curve at $(\wp(z), \wp'(z))$ (and if $z_1 = z_2 = z_3 = z$ then $(\wp(z), \wp'(z))$ is a point of inflection). This is the well-known "secants-and-tangents" description of the "addition law" on $y^2 = P_L(X)$. More generally, for any field k of characteristic zero[1] and any cubic polynomial $P \in k[X]$ without multiple roots, one can use secants and tangents to the curve $Y^2 = P(X)$ to give an "addition law" for the k-rational points on the curve (together with a "point at infinity"). We shall see that if $k = \mathbf{C}$ and $P(X)$ is normalized to the form $4X^3 + aX + b$ then $P = P_L$ for some lattice L, on which we recover the addition formulas for $\wp$ and $\wp'$.

Exercises

1. Prove that if D, E are divisors on the same Riemann surface and $D - E$ is principal then $\Gamma(D) \cong \Gamma(E)$. [Divisors whose difference is principal are said to be *linearly equivalent*.]

2. Prove that if D is a divisor on a compact Riemann surface and $\deg(D) \leq 0$ then $\Gamma(D) = \{0\}$, unless D is principal, when $\Gamma(D)$ is one-dimensional.

3. Prove that if D is a divisor on $\mathbf{C}/L$ of degree $d > 0$ then $\Gamma(D)$ has dimension d.

On $\mathbf{P}^1(\mathbf{C})$, a divisor D of degree $d \geq 0$ has $\dim(\Gamma(D)) = d + 1$. This and Exercise 3 are special cases of the Riemann-Roch theorem.

[1] It is enough for k not to have characteristic 2. When k has characteristic 3, the general elliptic curve over k is still $y^2 = P(X)$, but we can no longer assume that P has X^2 coefficient zero.