COMPLEX TORI

This writeup gives a quick sketch of results about complex tori, also known as complex elliptic curves for reasons to be explained in another writeup.

1. Definition

A *lattice in* $\mathbb{C}$ is a set $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\{\omega_1, \omega_2\}$ a basis for $\mathbb{C}$ over $\mathbb{R}$. We make the normalizing convention $\omega_1/\omega_2 \in \mathcal{H}$, but this still does not specify a basis given a lattice. Instead,

Lemma 1.1. *Consider two lattices* $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ *and* $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ *with* $\omega_1/\omega_2 \in \mathcal{H}$ *and* $\omega_1'/\omega_2' \in \mathcal{H}$*. Then* $\Lambda' = \Lambda$ *if and only if*

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \quad \textit{for some} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Proof. Exercise. □

A *complex torus* is a quotient of the complex plane by a lattice,

$$\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}.$$

Algebraically a complex torus is an Abelian group under the addition it inherits from $\mathbb{C}$. Geometrically a complex torus is a parallelogram spanned by $\{\omega_1, \omega_2\}$ with its sides identified in opposing pairs. Identifying one pair of sides rolls the parallelogram into a tube, and then identifying the other pair bends the tube into a torus. But the flat model of the complex torus with neighborhoods extending across the sides better illustrates that every complex torus is a *Riemann surface*, roughly meaning a connected set that looks like the complex plane $\mathbb{C}$ in the small.

The notion of a holomorphic map makes sense for Riemann surfaces since it is local. Any holomorphic map between compact Riemann surfaces is either a surjection or a map to one point. To see this, suppose X and Y are compact Riemann surfaces and $f : X \longrightarrow Y$ is holomorphic. Since f is continuous and X is compact and connected, so is the image $f(X)$, making $f(X)$ closed. Unless f is constant f is open by the Open Mapping Theorem of complex analysis, applicable to Riemann surfaces since it is a local result, making $f(X)$ open as well. So $f(X)$ is either a single point or a connected, open, closed subset of the connected set Y, i.e., all of Y. As a special case of this, any nonconstant holomorphic map from one complex torus to another is a surjection.

2. Maps Between Tori: Homomorphisms, Isomorphisms, Isogenies

Proposition 2.1. *Suppose* $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ *is a holomorphic map between complex tori. Then there exist complex numbers* m, b *with* $m\Lambda \subset \Lambda'$ *such that* $\varphi(z + \Lambda) = mz + b + \Lambda'$*. The map is invertible if and only if* $m\Lambda = \Lambda'$*.*

Proof. (Sketch.) The key is to lift φ to a holomorphic map $\tilde{\varphi} : \mathbb{C} \longrightarrow \mathbb{C}$ by using topology. (The plane is the so-called *universal covering space* of the torus—see a topology text for the definition and the relevant lifting theorem.) With the map lifted, consider for any $\lambda \in \Lambda$ the function $f_\lambda(z) = \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z)$. Since $\tilde{\varphi}$ lifts a map between the quotients, the continuous function f_λ maps to the discrete set Λ' and is therefore constant. Differentiating gives $\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z)$. Thus $\tilde{\varphi}'$ is holomorphic and Λ-periodic, making it bounded and therefore constant by Liouville's Theorem. Now $\tilde{\varphi}$ is a first degree polynomial $\tilde{\varphi}(z) = mz + b$, and again since this lifts a map between quotients, necessarily $m\Lambda \subset \Lambda'$. The original map thus has the form asserted in the proposition. If the containment $m\Lambda \subset \Lambda'$ is proper then φ is not injective: some $z \in \Lambda'$ satisfies $z/m \notin \Lambda$ but $\varphi(z/m + \Lambda) = b + \Lambda' = \varphi(\Lambda)$. If $m\Lambda = \Lambda'$ then $(1/m)\Lambda' = \Lambda$ and the map $\psi : \mathbb{C}/\Lambda' \longrightarrow \mathbb{C}/\Lambda$ given by $\psi(w + \Lambda') = (w-b)/m + \Lambda$ inverts φ. □

Corollary 2.2. *Suppose $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is a holomorphic map between complex tori, $\varphi(z+\Lambda) = mz + b + \Lambda'$ with $m\Lambda \subset \Lambda'$. Then the following are equivalent:*

1. *φ is a group homomorphism,*
2. *$b \in \Lambda'$, so $\varphi(z+\Lambda) = mz + \Lambda'$,*
3. *$\varphi(0) = 0$.*

In particular, there exists a nonzero holomorphic group homomorphism between the complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if and only if there exists some nonzero $m \in \mathbb{C}$ such that $m\Lambda \subset \Lambda'$, and there exists a holomorphic group isomorphism between the complex tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ if and only if there exists some $m \in \mathbb{C}$ such that $m\Lambda = \Lambda'$.

Proof. Exercise. □

For one isomorphism of particular interest, start from an arbitrary lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\omega_1/\omega_2 \in \mathcal{H}$. Let $\tau = \omega_1/\omega_2$ and let $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$. Then since $(1/\omega_2)\Lambda = \Lambda_\tau$, Corollary 2.2 shows that the map $\varphi_\tau : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda_\tau$ given by $\varphi(z+\Lambda) = z/\omega_2 + \Lambda_\tau$ is an isomorphism. This shows that every complex torus is isomorphic to a complex torus whose lattice is generated by a complex number $\tau \in \mathcal{H}$ and by 1. This τ is not unique, but if $\tau' \in \mathcal{H}$ is another such number then $\tau' = \omega_1'/\omega_2'$ where $\Lambda = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$, and so by Lemma 1.1 $\tau' = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Thus each complex torus determines a point $\tau \in \mathcal{H}$ up to the action of $\mathrm{SL}_2(\mathbb{Z})$. In fact the isomorphism classes of complex tori biject to the orbits $\mathrm{SL}_2(\mathbb{Z})\tau$ in $\mathcal{H}$.

Definition 2.3. *A nonzero holomorphic homomorphism between complex tori is called an* ***isogeny****.*

In particular, every holomorphic isomorphism is an isogeny. Every isogeny surjects and has finite kernel—the kernel is finite because it is discrete (otherwise complex analysis shows that the map is zero) and complex tori are compact.

Multiply-by-integer maps are isogenies but not isomorphisms. For any positive integer N and lattice Λ consider the map

$$[N] : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda, \qquad z + \Lambda \mapsto Nz + \Lambda.$$

This is an isogeny since $N\Lambda \subset \Lambda$. Its kernel, the points $z + \Lambda \in \mathbb{C}/\Lambda$ such that $[N](z+\Lambda) = 0$, is the set of *N-torsion points of* $\mathbb{C}/\Lambda$, a subgroup isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Letting E denote the torus $\mathbb{C}/\Lambda$ (for reasons to be explained soon), this subgroup is denoted $E[N]$.

Cyclic quotient maps are also isogenies but not isomorphisms. Let $\mathbb{C}/\Lambda$ be a complex torus, let N be a positive integer, and let C be a cyclic subgroup of $E[N]$ isomorphic to $\mathbb{Z}/N\mathbb{Z}$. The elements of C are cosets $\{c + \Lambda\}$ and so as a set C

forms a superlattice of Λ. Slightly abusing notation we use the same symbol for the subgroup and the superlattice. Then the cyclic quotient map

$$\pi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/C, \qquad z+\Lambda \mapsto z+C$$

is an isogeny with kernel C.

In fact every isogeny is a composition of the examples already given. To see this, consider an arbitrary isogeny

$$\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda', \qquad z+\Lambda \mapsto mz+\Lambda'$$

and let K denote its kernel, the finite subgroup $K = m^{-1}\Lambda'/\Lambda$ of $\mathbb{C}/\Lambda$ also viewed as the superlattice $K = m^{-1}\Lambda'$ of Λ. If N is the order of K as a subgroup then $K \subset E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, and so by the theory of finite Abelian groups $K \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nn'\mathbb{Z}$ for some positive integers n and n'. The multiply-by-n isogeny $[n]$ of $\mathbb{C}/\Lambda$ takes K to a cyclic subgroup nK isomorphic to $\mathbb{Z}/n'\mathbb{Z}$, and then the quotient isogeny π from $\mathbb{C}/\Lambda$ to $\mathbb{C}/nK$ has kernel nK. Follow this by the map $\mathbb{C}/nK \longrightarrow \mathbb{C}/\Lambda'$ given by $z+nK \mapsto (m/n)z + (m/n)nK$, now viewing nK as a lattice in $\mathbb{C}$. This map makes sense and is an isomorphism since $(m/n)nK = mK = \Lambda'$. The composition of the three maps is $z+\Lambda \mapsto nz+\Lambda \mapsto nz+nK \mapsto mz+\Lambda' = \varphi(z+\Lambda)$. That is, the general isogeny is a composition as claimed,

$$\varphi : \mathbb{C}/\Lambda \xrightarrow{[n]} \mathbb{C}/\Lambda \xrightarrow{\pi} \mathbb{C}/nK \xrightarrow{\sim} \mathbb{C}/\Lambda'.$$

A very similar argument shows that isogeny is an equivalence relation. Suppose that $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is an isogeny. Thus $\varphi(z+\Lambda) = mz+\Lambda'$ where $m \neq 0$ and $m\Lambda \subset \Lambda'$. By the theory of finite Abelian groups there exists a basis $\{\omega_1, \omega_2\}$ of Λ' and positive integers n_1, n_2 such that $\{n_1\omega_1, n_2\omega_2\}$ is a basis of $m\Lambda$. It follows that $n_1n_2\Lambda' \subset m\Lambda$ and therefore $(n_1n_2/m)\Lambda' \subset \Lambda$. Thus there is a *dual isogeny* $\hat{\varphi} : \mathbb{C}/\Lambda' \longrightarrow \mathbb{C}/\Lambda$ back in the other direction, $\hat{\varphi}(z+\Lambda') = (n_1n_2/m)z+\Lambda$. Note that $(\hat{\varphi} \circ \varphi)(z+\Lambda) = n_1n_2z+\Lambda$, i.e., the isogeny followed by its dual is multiplication by a positive integer. The integer n_1n_2 in question is the degree of the original isogeny since $\{\omega_1/m, \omega_2/m\}$ is a basis of $\ker(\varphi)$ and $\{n_1\omega_1/m, n_2\omega_2/m\}$ is a basis of Λ, making $\ker(\varphi) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ and showing that φ is n_1n_2-to-1. That is,

$$\hat{\varphi} \circ \varphi = [\deg(\varphi)].$$

This condition specifies $\hat{\varphi}$ uniquely since φ surjects. Since the map $[\deg(\varphi)]$ has degree $(\deg(\varphi))^2$ and the degree of a composition is the product of the degrees, the dual isogeny has degree $\deg(\hat{\varphi}) = \deg(\varphi)$. The dual isogeny of a multiply-by-integer map is itself. The dual isogeny of a cyclic quotient isogeny quotients the torus in a second direction by a cyclic group of the same order to restore its shape and then expands it back to full size. The dual isogeny of an isomorphism is its inverse. The dual of a composition of isogenies is the composition of the duals in the reverse order. If φ is an isogeny and $\hat{\varphi}$ is its dual then the formulas $\varphi(z+\Lambda) = mz+\Lambda'$, $\hat{\varphi}(z'+\Lambda') = (\deg(\varphi)/m)z'+\Lambda$ show that also

$$\varphi \circ \hat{\varphi} = [\deg(\varphi)] = [\deg(\hat{\varphi})],$$

so that φ is in turn the dual isogeny of its dual $\hat{\varphi}$. Isogeny of complex tori, rather than isomorphism, will turn out to be the appropriate equivalence relation in the context of modular forms.

If $\varphi_1, \varphi_2 : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ are isogenies, and $\varphi_1 + \varphi_2 \neq 0$ so that their sum is again an isogeny, then the dual of the sum is the sum of their duals. To see this, let $\varphi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ be an isogeny. Thus $\varphi(z+\Lambda) = mz + \Lambda'$ where $m \neq 0$ and $m\Lambda \subset \Lambda'$. Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\omega_1/\omega_2 \in \mathcal{H}$, and similarly for Λ'. Consequently

$$\begin{bmatrix} m\omega_1 \\ m\omega_2 \end{bmatrix} = \alpha \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} \quad \text{for some } \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Homogenizing this equality gives $\omega_1/\omega_2 = \alpha(\omega_1'/\omega_2')$ where now α acts as a fractional linear transformation, showing that $\det\alpha \neq 0$ and hence $\det\alpha > 0$ because in general $\mathrm{Im}\,(\alpha(\tau)) = \det\alpha \cdot \mathrm{Im}\,(\tau)\,/|j(\alpha,\tau)|^2$ for $\alpha \in \mathrm{GL}_2(\mathbb{R})$. This justifies the last step of the calculation

$$\deg(\varphi) = |\ker(\varphi)| = [m^{-1}\Lambda' : \Lambda] = [\Lambda' : m\Lambda] = \det\alpha.$$

Since $\hat\varphi \circ \varphi = [\deg(\varphi)]$ and the matrix of a composition is the right-to-left product of the matrices, the dual isogeny must induce the matrix

$$\hat\alpha = \det\alpha \cdot \alpha^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

and conversely this matrix determines the dual isogeny. Now let φ_1 and φ_2 be isogenies from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda'$ with $\varphi_1 + \varphi_2 \neq 0$. Their sum $(\varphi_1+\varphi_2)(z+\Lambda) = (m_1+m_2)z + \Lambda'$ gives rise to the matrix

$$\alpha_1 + \alpha_2 = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix},$$

and so correspondingly the dual isogeny of the sum is determined by the matrix

$$\begin{bmatrix} d_1+d_2 & -b_1-b_2 \\ -c_1-c_2 & a_1+a_2 \end{bmatrix} = \hat\alpha_1 + \hat\alpha_2,$$

the sum of the matrices determining the dual isogenies. This proves the claim at the beginning of the paragraph,

$$\widehat{\varphi_1 + \varphi_2} = \hat\varphi_1 + \hat\varphi_2 \quad \text{if } \varphi_1 + \varphi_2 \neq 0. \tag{1}$$

For one more example, some complex tori have endomorphisms other than the multiply-by-N maps $[N]$, in which case they have *complex multiplication.* Let $\tau = \sqrt{d}$ for some squarefree $d \in \mathbb{Z}^-$ such that $d \equiv 2, 3 \pmod 4$, or let $\tau = (-1+\sqrt{d})/2$ for squarefree $d \in \mathbb{Z}^-$, $d \equiv 1 \pmod 4$. Then the set $\mathcal{O} = \tau\mathbb{Z} \oplus \mathbb{Z}$ is a ring. (Readers with background in number theory will recognize it as the ring of integers in the imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$.) Let Λ be any ideal of $\mathcal{O}$ and let m be any element of $\mathcal{O}$. Then $m\Lambda \subset \Lambda$, so multiplying by m gives an endomorphism of $\mathbb{C}/\Lambda$. In particular, the ring of endomorphisms of $\mathbb{C}/\Lambda_i$ is isomorphic to $\Lambda_i = i\mathbb{Z}\oplus\mathbb{Z}$ rather than to $\mathbb{Z}$, and similarly for the ring of endomorphisms of $\mathbb{C}/\Lambda_{\zeta_3}$ where $\zeta_3 = e^{2\pi i/3}$.

3. The Weil Pairing

Let Λ be a lattice. The N-torsion subgroup of the additive torus group $\mathbb{C}/\Lambda$,

$$E[N] = \{P \in \mathbb{C}/\Lambda : [N]P = 0\} = \langle \omega_1/N + \Lambda \rangle \times \langle \omega_2/N + \Lambda \rangle,$$

is analogous to the N-torsion subgroup of the multiplicative circle group $\mathbb{C}^*/\mathbb{R}^+ \cong \{z \in \mathbb{C} : |z| = 1\} \cong \mathbb{R}/\mathbb{Z}$, the complex Nth roots of unity

$$\boldsymbol{\zeta}_N = \{z \in \mathbb{C} : z^N = 1\} = \langle e^{2\pi i/N} \rangle.$$

A sort of inner product exists on $E[N]$ with values in $\boldsymbol{\zeta}_N$, the *Weil pairing*

$$e_N : E[N] \times E[N] \longrightarrow \boldsymbol{\zeta}_N.$$

To define this, let P and Q be points in $E[N]$, possibly equal. If $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $\omega_1/\omega_2 \in \mathcal{H}$ then

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \gamma \begin{bmatrix} \omega_1/N + \Lambda \\ \omega_2/N + \Lambda \end{bmatrix} \quad \text{for some } \gamma \in \mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$$

since $\omega_1/N + \Lambda$ and $\omega_2/N + \Lambda$ generate $E[N]$. The Weil pairing of P and Q is

$$e_N(P, Q) = e^{2\pi i \det \gamma / N}.$$

This makes sense even though $\det \gamma$ is defined only modulo N. It is independent of how the basis $\{\omega_1, \omega_2\}$ is chosen (and once the basis is chosen the matrix γ is uniquely determined since its entries are reduced modulo N), remembering the normalization $\omega_1/\omega_2 \in \mathcal{H}$ (exercise). If P and Q generate $E[N]$ then the matrix γ lies in the group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ of invertible 2-by-2 matrices with entries in $\mathbb{Z}/N\mathbb{Z}$, making $\det \gamma$ invertible modulo N and $e_N(P, Q)$ therefore a primitive complex Nth root of unity. See parts (b–d) of the following exercise for more properties of the Weil pairing, in particular that the Weil pairing is preserved under isomorphisms of complex tori.

Exercise (a) Show that the Weil pairing is independent of which basis $\{\omega_1, \omega_2\}$ is used, provided $\omega_1/\omega_2 \in \mathcal{H}$.

(b) Show that the Weil pairing is bilinear, alternating, and nondegenerate. (Remember that the group $\boldsymbol{\zeta}_N$ is multiplicative.)

(c) Show that the Weil pairing is compatible with N. This means that for positive integers N and d, the diagram

$$\begin{tikzcd}
E[dN] \times E[dN] \arrow[r, "e_{dN}(\cdot,\cdot)"] \arrow[d, "d(\cdot{,}\cdot)"'] & \boldsymbol{\zeta}_{dN} \arrow[d, "\cdot^d"] \\
E[N] \times E[N] \arrow[r, "e_N(\cdot,\cdot)"] & \boldsymbol{\zeta}_N
\end{tikzcd}$$

commutes, where the vertical maps are suitable multiplications by d.

(d) Let Λ and Λ' be lattices with $m\Lambda = \Lambda'$ for some $m \in \mathbb{C}$. Show that the isomorphism of complex elliptic curves $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}/\Lambda'$ given by $z + \Lambda \mapsto mz + \Lambda'$ preserves the Weil pairing.