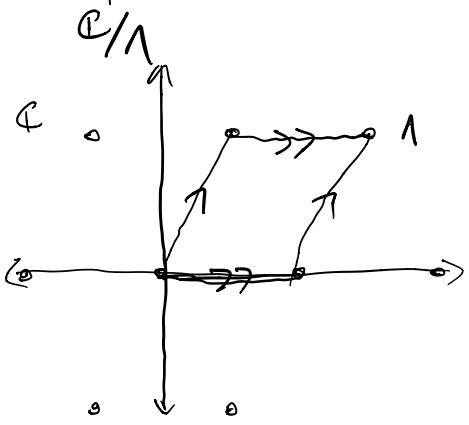
Elliptic curves

Two perspectives:

- Algebraic geometry → An elliptic curve is a nonsingular projective curve with a compatible grp structure
- Riemann surfaces → An E.C. is a compact R.S. with a compatible grp struct.

→ An E.C. is a complex torus



→ ——— is a nonsingular projective curve of genus 1 and a distinguished pt.

→ ——— is a projective curve of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $4a^3 + 27b^2 \neq 0$

(char $\neq 2, 3$)

E/K ell. curve over K

if $K \subseteq \mathbb{C}$, $E(\mathbb{C})$ is a R.S.

if $E = \mathbb{C}/\Lambda$, then $\exists a, b \in \mathbb{C}$ s.t. $E \cong E'(\mathbb{C})$, $E'/\mathbb{C}$

sometimes E'/K $K \subseteq \mathbb{C}$

Source: Diamond + Shurman §1.3, 1.4.

Riemann surfaces

Recall: a manifold is something that "looks locally" like $\mathbb{R}^n$

a curve looks locally like $\mathbb{R}$

Defn A **Riemann surface** is a connected Hausdorff topological space X together with an **atlas** $\{(U_\alpha, \varphi_\alpha)\}_\alpha$ where

- $\{U_\alpha\}$ is a covering of X by open sets U_α
- $\varphi_\alpha : U_\alpha \longrightarrow V_\alpha$ is a homeomorphism of U_α with some open $V_\alpha \subseteq \mathbb{C}$
- the **transition maps** $\varphi_\beta \circ \varphi_\alpha^{-1} : V_\alpha \longrightarrow V_\beta$ are holomorphic

Each $(U_\alpha, \varphi_\alpha)$ is called a **coordinate neighborhood**.

Ex. $\mathbb{C}$. Atlas $= \{(\mathbb{C}, id_{\mathbb{C}})\}$. Similarly, any open $U \subseteq \mathbb{C}$ is a R.S.

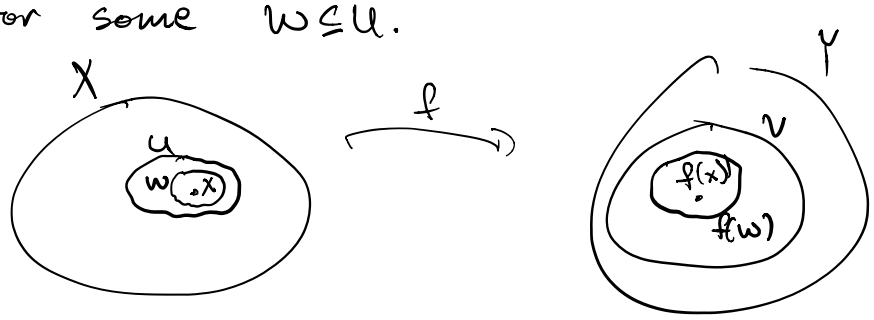
Ex. $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ **compact** R.S.

Defn A **(holomorphic) map of R.S.'s** $f : X \longrightarrow Y$

is a function so that at each $x \in X$, we have coord. nbhds (U, φ_U) of x and (V, φ_V) of $f(x) \in Y$

s.t. $\varphi_V \circ f \circ \varphi_U^{-1}\big|_{\varphi_U(W)} : \varphi_U(W) \longrightarrow \mathbb{C}$ is holo.

for some $W \subseteq U$.



Ex. If $f: U \longrightarrow \mathbb{C}$ is holo. then f is map of R.S.'s.
$\cap\!|$
$\mathbb{C}$

Ex. If $f: U \longrightarrow \mathbb{C} \cup \{\infty\} = \mathbb{P}^1$ is meromorphic then
$\cap\!|$
$\mathbb{C}$
it is a map of R.S.'s.

Locally, maps of R.S.'s all look like $z \longmapsto z^n$ $(n \geq 1)$.

Prop Let $f: X \longrightarrow Y$ be a map of R.S.'s. For every $x \in X$, there are nbhds $x \in U \subseteq X$, $f(x) \in V \subseteq Y$ and isomorphisms of R.S.'s

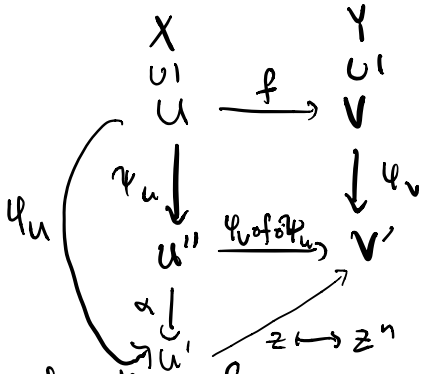
$$\varphi_U : U \longrightarrow U' \subseteq \mathbb{C}$$
$$\varphi_V : V \longrightarrow V' \subseteq \mathbb{C}$$

s.t.

$$\varphi_V \circ f \circ \varphi_U^{-1}(z) = \text{either } 0 \text{ or } z^n \text{ for some } n \geq 1.$$

Pf. Let (U, φ_U), (V, φ_V) be coord. nbhds of x, $f(x)$. After composing w/ translations, can assume that

$$\varphi_U(x) = 0$$
$$\varphi_V(f(x)) = 0.$$



$$\varphi_U : U \longrightarrow U'' \subseteq \mathbb{C}$$
$$\varphi_V : V \longrightarrow V' \subseteq \mathbb{C}$$

and $\varphi_V \circ f \circ \varphi_U^{-1}$ is holo. Thus, of the form

$$\varphi_V \circ f \circ \varphi_U^{-1}(z) = \begin{cases} 0, & \text{or} \\ a_n z^n + a_{n+1} z^{n+1} + \cdots, & a_n \neq 0, \ n \geq 1. \end{cases}$$

$$= z^n (a_n + a_{n+1} z + \cdots)$$

$$= z^n g(z) \qquad g(0) \neq 0, \ g \text{ is holo.}$$

$r(z) = g(z)^{1/n}$ is holo, possibly after shrinking U, U'' further.

Let $\alpha(z) = z\, r(z)$: holo $\alpha'(0) = r(0) \neq 0$.

$$\alpha(z)^n = \varphi_V \circ f \circ \varphi_U^{-1}$$

and α is a bijection on some nbhd of 0. Shrinking U, U'' further, $\alpha : U'' \xrightarrow{\sim} U'$.

Done with $\psi_u = \alpha \circ \gamma_u$. □

Thm (open mapping thm) If $f: X \to Y$ is a nonconstant map of R.S.'s, then whenever $U \subseteq X$ is open, so is $f(U) \subseteq Y$.

Pf. True for $z \mapsto z^n$ $n \geq 1$. □

Cor If $f: X \to Y$ is a nonconstant map of compact R.S.'s then f is surjective.

Pf. $f(X) \subseteq Y$ is open and closed. □

Cor. (Liouville's thm) A nonconstant holo. map $\mathbb{C} \to \mathbb{C}$ is unbounded.

Pf.

$$\begin{array}{ccc} f: & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & \cap | & & \cap | \\ \tilde{f}: & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ & \cup & & \cup \\ & \infty & \longmapsto & \infty \end{array}$$

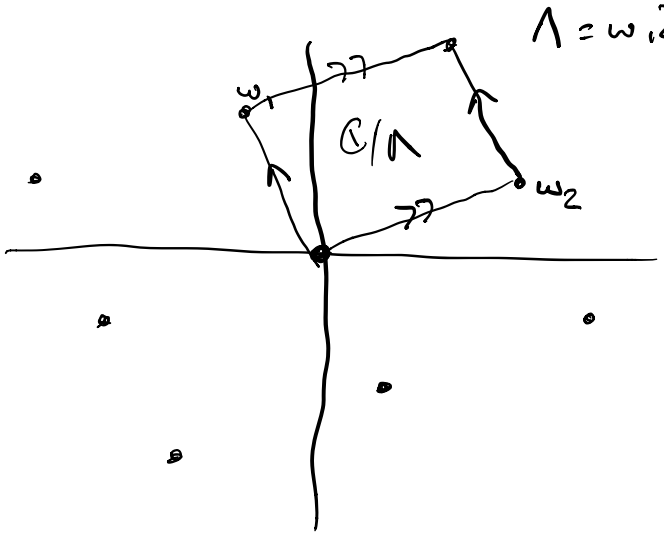
□

Complex tori

The only R.S.'s we'll care about are the compact R.S.'s $\mathbb{P}^1$, and the following

Defn A lattice in $\mathbb{C}$ is a group

$$\Lambda = w_1\mathbb{Z} + w_2\mathbb{Z} \quad \text{where } \{w_1, w_2\} \text{ is a basis for } \mathbb{C} \text{ over } \mathbb{R}.$$



Convention: $\frac{w_1}{w_2} \in \mathcal{H}$ (i.e. $\mathrm{Im}(w_1/w_2) > 0$).

Defn A complex torus (a complex elliptic curve)

is a R.S.'s of the form $\mathbb{C}/\Lambda$ where $\Lambda \subseteq \mathbb{C}$ is a lattice.

Note: $\mathbb{C}/\Lambda$ is a group!

Exercise. Prove that $\mathbb{C}/\Lambda$ is a compact R.S., and show that the maps

$$+z_0 : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda \qquad z \longmapsto z + z_0$$

$$- : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda \qquad z \longmapsto -z$$

are holo. isomorphisms of R.S.'s.

What do maps between cmplx tori look like?

Fact: Every holo. map $f: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ lifts to a holo. map $\tilde{f}: \mathbb{C} \longrightarrow \mathbb{C}$ with $f(\Lambda) \subseteq \Lambda'$.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{f}} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda' \end{array}$$

Prop Let $f: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ be a map. There exist $m, b \in \mathbb{C}$ s.t.

$$f(z+\Lambda) = mz + b + \Lambda'$$

and $m\Lambda \subseteq \Lambda'$.

Moreover, f is invertible $\iff m\Lambda = \Lambda'$.

Pf. Lift f to $\tilde{f}: \mathbb{C} \longrightarrow \mathbb{C}$.

Let $\lambda \in \Lambda$, and define $\varphi = \tilde{f}(z+\lambda) - \tilde{f}(z)$.

φ is holo., and its image is contained in Λ'. Thus $\varphi =$ constant!

Thus $\tilde{f}'(z+\lambda) = \tilde{f}'(z)$. $\tilde{f}'$ is holo, and periodic under Λ, hence bounded. Thus $\tilde{f}'$ is constant, and

$$\tilde{f}(z) = mz + b, \quad m, b \in \mathbb{C}.$$

$f(z+\Lambda) = mz + b + \Lambda'$ and since $f(\Lambda) \subseteq \Lambda'$, so also $m\Lambda \subseteq \Lambda'$.

For the "moreover":

f is invertible $\iff$ f is bijective

$\iff$ $m \neq 0$ and f is inj.

$\iff$ $m \neq 0$ and $\left(mz' - mz \in \Lambda' \iff z' - z \in \Lambda \right)$

$\iff$ $m \neq 0$ and $m\Lambda = \Lambda'$

$\iff$ $m\Lambda = \Lambda'$. $\square$.