Problem set 1: Reminder on Riemann surfaces

Exercise 1 (Group actions).

(a) Suppose $D \subset \mathbb{P}^1(\mathbb{C})$ is a domain and let $G < \mathrm{Aut}(\mathbb{P}^1(\mathbb{C})) = \mathrm{PGL}(2, \mathbb{C})$ be such that

- $g(D) = D$ for all $g \in G$
- if $g \in G \setminus \{e\}$ then the fixed points of g lie outside of D, i.e. the action on D is *free*,
- for each compact subset $K \subset D$, the set

$$\{g \in G;\ g(K) \cap K \neq \emptyset\}$$

  is finite. That is, the action on D is *properly discontinuous*.

Show that the quotient space $G\backslash D$ can be equipped with the structure of a connected Riemann surface (using local inverses to the projection map $\pi : D \to G\backslash D$ as charts).

Solution: First of all, since D is connected and π is continuous, $G\backslash D$ is connected.

In order to show that $G\backslash D$ is Hausdorff, we consider two distinct points

$$\pi(z_1) \neq \pi(z_2) \in G\backslash D$$

where z_1 and z_2 are two pre-images in D. Define

$$A_n = \{w \in D;\ |w - z_1| < r/n\} \quad \text{and} \quad B_n = \{w \in D;\ |w - z_2| < r/n\},$$

where $r > 0$ is small enough so that

$$K = \overline{A_1} \cup \overline{B_1} \subset D.$$

Now, suppose that for all $n \geq 1$ we have

$$\pi(A_n) \cap \pi(B_n) \neq \emptyset$$

This means that we can find some sequence $a_n \in A_n$ and $g_n \in G$ so that

$$g_n(a_n) \in B_n$$

for all $n \in \mathbb{N}$. This means that

$$\emptyset \neq g_n(A_n) \cap B_n \subset g_n(K) \cap K$$

for all $n \in \mathbb{N}$ and hence by the third assumption, the set $\{g_n\}_{n\in\mathbb{N}}$ is finite. This means that there is a subsequence so that $g_n = g$ for some fixed $g \in G$ and all n large enough

$$z_2 = \lim_{n\to\infty} g_n(a_n) = \lim_{n\to\infty} g(a_n) = g(z_1),$$

which contradicts $\pi(z_1) \neq \pi(z_2)$ and hence proves that $G\backslash D$ is Hausdorff.

All that remains is to find an atlas. To this end, select a precompact open disk $K_z \subset D$ around each $z \in D$. By assumptions (2) and (3) we can choose K_z small enough so that no non-trivial translate $g(K_z)$ intersects it. This implies that the map

$$\pi|_{K_z} : K_z \to G\backslash D$$

is a homeomorphism onto its image. So we set

$$U_z = \pi(K_z) \quad \text{and} \quad \varphi_z = (\pi|_{K_z})^{-1} : U_z \to D.$$

This means that the transition maps are of the form

$$\varphi_z \circ \varphi_w^{-1} = (\pi|_{K_z})^{-1} \circ (\pi|_{K_w}).$$

Given any element ζ in the domain of this map, we have

$$\varphi_z \circ \varphi_w^{-1}(\zeta) = g(\zeta) =: \xi$$

for some $g \in G$ and $\xi \in D$. Near ζ we have $\pi = \pi|_{K_w}$ while near ξ we have $\pi = \pi|_{K_z}$. Since $\pi = \pi \circ g$ for all $g \in G$, we obtain

$$\pi|_{K_z} = \pi|_{K_w} \circ g$$

and hence

$$\varphi_z \circ \varphi_w^{-1} = g$$

near ζ, which is holomorphic.

(b) Show that $G < \mathrm{PGL}(2, \mathbb{C})$ is discrete (with respect to the induced topology) if and only if the identity element $e \in G$ is isolated.

Solution: G is discrete if and only if for all $g \in G$ there exists some open set $U \subset \mathrm{PGL}(2, \mathbb{C})$ such that $U \cap G = \{g\}$. In particular, if G is discrete then the identity is isolated.

Conversely, if the identity is isolated, there is some open set $U \subset \mathrm{PGL}(2, \mathbb{C})$ such that $U \cap G = \{e\}$. Left multiplication by $g \in G$ is a homeomorphism $\mathrm{PGL}(2, \mathbb{C}) \to \mathrm{PGL}(2, \mathbb{C})$, so gU is an open set. This means that

$$\{g\} = g\{e\} = g(U \cap G) = gU \cap G.$$

Exercise 2 (Hyperbolic geometry). Let $\mathbb{H}^2 = \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$.

(a) Show that

$$\{g \in \mathrm{PGL}(2,\mathbb{C});\ g(\mathbb{H}^2) = \mathbb{H}^2\} = \mathrm{PSL}(2,\mathbb{R}).$$

Remark: $\mathrm{PGL}(2,\mathbb{C}) = \mathrm{PSL}(2,\mathbb{C})$ so we can freely switch between the two. However $\mathrm{PSL}(2,\mathbb{R}) < \mathrm{PGL}(2,\mathbb{R})$ is a proper subgroup, the latter contains $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, whereas the former does not.

Solution: First we show that $\mathrm{PSL}(2,\mathbb{R})$ preserves $\mathbb{H}^2$. Suppose $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{R})$ and $z \in \mathbb{H}^2$. Then

$$\begin{aligned} \mathrm{Im}(g(z)) &= \frac{1}{2i}\left(\frac{az+b}{cz+d} - \frac{a\overline{z}+b}{c\overline{z}+d}\right) \\ &= \frac{1}{2i}\frac{(ad-bc)(z-\overline{z})}{|cz+d|^2} \\ &= \frac{\mathrm{Im}(z)}{|cz+d|^2} \\ &> 0. \end{aligned}$$

So $\mathrm{PSL}(2,\mathbb{R})$ indeed preserves $\mathbb{H}^2$.

On the other hand, if g preserves $\mathbb{H}^2$, it also needs to presrve $\partial\mathbb{H}^2 = \mathbb{R} \cup \{\infty\}$. Write $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}(2,\mathbb{C})$.

If $c, d \neq 0$ and $c \neq -d$, we can normalize the matrix such that $d = 1$. We then get that

$$g(0) = b, \quad g(\infty) = \frac{a}{c} \quad \text{and} \quad g(1) = \frac{a+b}{c+1}$$

are three distinct elements of $\mathbb{R}$.

$$\begin{aligned} 0 = \mathrm{Im}(g(1)) &= \frac{1}{2i}\frac{(a+b)\overline{(c+1)} - \overline{(a+b)}(c+1)}{|c+1|^2} \\ &= \frac{1}{2i}\frac{(g(\infty)c + g(0))\overline{(c+1)} - (g(\infty)\overline{c} + g(0))(c+1)}{|c+1|^2} \\ &= \frac{g(\infty)(c-\overline{c}) + g(0)(\overline{c}d - c\overline{d})}{|c+d|^2} \\ &= \frac{(g(\infty) - g(0))(c-\overline{c})}{|c+1|^2} \end{aligned}$$

So c and hence a are real, so $g \in \mathrm{PGL}(2,\mathbb{R})$. By computing $\mathrm{Im}(g(z))$ as before, we prove that $ad - bc > 0$. We can divide by the root of the determinant so that $ad - bc = 1$.

If $c, d \neq 0$ and $c = -d$, we can normalize the matrix such that $d = 1$ and $c = -1$. We get that

$$g(0) = b, \quad g(\infty) = -a$$

are both real. Moreover, because $\mathrm{Im}(g(z))$ needs to be positive, we again obtain that $ad - bc > 0$, which again allows us to divide by the root of the determinant such that $ad - bc = 1$.

<u>If $c = 0$</u>, then $d \neq 0$ and we can normalize such that $d = 1$. This means that

$$g(0) = b \in \mathbb{R}, \quad \text{and} \quad g(1) = a + b \in \mathbb{R}$$

so both $a, b \in \mathbb{R}$. Again using that $\mathrm{Im}(g(z)) > 0$ and normalizing, we obtain that $g \in \mathrm{PSL}(2, \mathbb{R})$.

<u>If $d = 0$</u>, then $c \neq 0$ and we can normalize such that $c = 1$. This means that

$$g(\infty) = a \in \mathbb{R}, \quad \text{and} \quad g(1) = a + b \in \mathbb{R},$$

so both $a, b \in \mathbb{R}$. Using that $\mathrm{Im}(g(z)) > 0$ and normalizing one last time, we obtain that $g \in \mathrm{PSL}(2, \mathbb{R})$.

(b) We're going to prove the Iwasawa decomposition for $\mathrm{SL}(2, \mathbb{R})$. Namely, if we set

$$K = \mathrm{SO}(2, \mathbb{R}), \quad A = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix} ; \lambda > 0 \right\} \quad \text{and} \quad N = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} ; \ t \in \mathbb{R} \right\},$$

then $\mathrm{SL}(2, \mathbb{R}) = KAN$, i.e. for every matrix $g \in \mathrm{SL}(2, \mathbb{R})$, there exist a unique $k \in K$, $a \in A$ and $n \in N$ such that $g = kan$.

- Let (e_1, e_2) denote the standard basis of $\mathbb{R}^2$ and set $v_i = ge_i$ for $i = 1, 2$. Moreover, set

$$w_1 = v_1, \quad w_2 = v_2 - \frac{\langle w_1, v_2 \rangle}{\langle w_1, w_1 \rangle} \cdot w_1,$$

where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^2$. Show that there exist $k \in O(2)$ and $a = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ with $\lambda, \mu > 0$ such that

$$k^{-1} w_i = a e_i, \quad i = 1, 2.$$

<u>Solution:</u> $\frac{w_1}{\|w_1\|}$ and $\frac{w_2}{\|w_2\|}$ form an orthonormal basis of $\mathbb{R}^2$ (the equations defining w_1 and w_2 are an application of the Gram-Schmidt procedure). In particular, there exists an element $k \in O(2)$ such that

$$k^{-1} \frac{w_i}{\|w_i\|} = e_i \quad \Longrightarrow \quad k^{-1} w_i = \|w_i\| \cdot e_i.$$

We can set $a = \begin{pmatrix} \|w_1\| & 0 \\ 0 & \|w_2\| \end{pmatrix}$.

- Show that there exists an $n \in N$ such that

$$g^{-1}w_i = n^{-1}e_i, \quad i = 1, 2$$

Solution: We have

$$g^{-1}w_1 = e_1 \quad \text{and} \quad g^{-1}w_2 = e_2 - \frac{\langle w_1, v_2 \rangle}{\langle w_1, w_1 \rangle} \cdot e_1.$$

So we can set $n = \begin{pmatrix} 1 & \frac{\langle w_1, v_2 \rangle}{\langle w_1, w_1 \rangle} \\ 0 & 1 \end{pmatrix}$.

- Conclude that $g = kan$ and show that $k \in K$ and $a \in A$.

Solution: We have

$$n\, g^{-1}w_i = e_i = a^{-1}k^{-1}w_i, \quad i = 1, 2.$$

Because (w_1, w_2) is a basis, this means that $g = kan$.
Moreover, we have

$$1 = \det(g) = \det(k)\det(a)\det(n) = \det(k)\det(a).$$

The determinant $\det(k) \in \{\pm 1\}$ and $\det(a) > 0$. This implies that $\det(k) = 1$ and hence that $\det(a) = 1$.

- Show that the decomposition $g = kan$ is unique.

Solution: Suppose $k_1a_1n_1 = k_2a_2n_2$. Then

$$k_2^{-1}k_1 = a_2n_2n_1^{-1}a_1^{-1} \in K \cap ANA.$$

Now we observe that

$$ANA = \left\{ \begin{pmatrix} \lambda & t \\ 0 & \lambda^{-1} \end{pmatrix};\ t \in \mathbb{R},\ \lambda > 0 \right\} = AN.$$

This implies that

$$K \cap ANA = \{e\}$$

and hence that $k_1 = k_2$ and

$$a_2^{-1}a_1 = n_2n_1^{-1} \in A \cap N = \{e\}$$

and thus that $a_1 = a_2$ and $n_1 = n_2$.

- Bonus: Prove the Iwasawa decomposition of $\mathrm{SL}(n, \mathbb{R})$.

Solution: The strategy is the same.

(c) Show that $\mathrm{PSL}(2,\mathbb{R})$ preserves the Riemannian metric

$$ds^2 = \frac{dx^2 + dy^2}{y^2} =: \frac{|dz|^2}{\mathrm{Im}(z)^2} \quad \text{at } z = x + iy \in \mathbb{H}^2.$$

Solution: We're first going to use 2-dimensional real differential geometry to prove that

$$f^*\left(\frac{|dz|^2}{\mathrm{Im}(z)^2}\right) = \left|\frac{df}{dz}(z)\right|^2 \frac{|dz|^2}{\mathrm{Im}(f(z))^2}$$

Writing $f(x+iy) = u(x+iy) + iv(x+iy)$ for two smooth real valued functions u, v and taking $p \in \mathbb{H}^2$, we obtain

$$\begin{aligned}(f^*dx)_p^2 = &\left(\left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial y}\right)^2\right)\bigg|_p \cdot (dx_p^2 + dy_p^2)\\ &+ \left(\frac{\partial u}{\partial x}\frac{\partial u}{\partial y} + \frac{\partial v}{\partial x}\frac{\partial v}{\partial y}\right)\bigg|_p \cdot dx_p \cdot dy_p.\end{aligned}$$

The fact that f is holomorphic (and hence satisfies the Cauchy–Riemann equations) means that the mixed term disappears.

Moreover, one computes that at $z = p$,

$$\left|\frac{\partial f}{\partial z}\right|^2 = \left|\frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right) f(z)\right|^2 = \left(\left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial y}\right)^2\right)\bigg|_p,$$

thus proving our original claim.

Now write $f(z) = (az+b)/(cz+d)$. A computation similar to the one in item (a) shows that $|f'(z)|/\mathrm{Im}(f(z)) = 1/\mathrm{Im}(z)$, thus proving that f preserves the metric.

(d) Prove that the geodesics in $\mathbb{H}^2$ are vertical lines and half circles orthogonal to $\mathbb{R}$.

Solution: Let us first try to compute the length between a pair of points ai and bi on the imaginary axis with $0 < a < b$. Let $\gamma : [0,1] \to \mathbb{H}^2$ be any smooth curve with $\gamma(0) = ai$ and $\gamma(1) = bi$. We will write $\gamma_1(t) = \mathrm{Re}(\gamma(t))$ and $\gamma_2(t) = \mathrm{Im}(\gamma(t))$. Then the length of γ is

$$\begin{aligned}\ell(\gamma) &= \int_0^1 \frac{1}{\gamma_2(t)}\sqrt{\left(\frac{\partial\gamma_1(t)}{\partial t}\right)^2 + \left(\frac{\partial\gamma_2(t)}{\partial t}\right)^2}\,dt\\ &\geq \int_0^1 \frac{1}{\gamma_2(t)}\left|\frac{\partial\gamma_2(t)}{\partial t}\right| dt\end{aligned}$$

with equality if and only if $\partial\gamma_1(t)/\partial t = 0$ for all $t \in [0,1]$. Furthermore

$$\int_0^1 \frac{1}{\gamma_2(t)}\left|\frac{\partial\gamma_2(t)}{\partial t}\right| dt \geq \int_0^1 \frac{1}{\gamma_2(t)}\frac{\partial\gamma_2(t)}{\partial t}dt$$

with equality if and only if $\partial\gamma_2(t)/\partial t \geq 0$ for all $t \in [0,1]$. Moreover, we may assume that the points where $\partial\gamma_2(t)/\partial t = 0$ are isolated, because intervals on which this derivative is 0 don't contribute to the integral. So γ_2 is strictly increasing and hence invertible. This implies that we can apply the substituion rule and get

$$\ell(\gamma) \geq \int_a^b \frac{1}{d} ds = \log(b/a).$$

Since (for example) the curve $\gamma(t) = ai + (b-a)it$ has $\ell(\gamma) = \log(b/a)$, we conclude that the distance between these points $\log(b/a)$ and the moreover, the unique geodesic segment between them lies on the vertical line.

Given two points $z, w \in \mathbb{H}^2$, we can map them onto the imaginary axis with a Möbius transformation $g \in \mathrm{PSL}(2,\mathbb{R})$. The distance between their images on the imaginary axis is uniquely realized by a segment σ on the imaginary axis. Since $\mathrm{PSL}(2,\mathbb{R})$ acts by isometries, the distance between z and w is uniquely realized by $g^{-1}\sigma$. Möbius transformations send lines and circles to lines and circles and moreover are confromal (they preserve angles. So the image of σ (lying on the image of the imaginary axis under g^{-1}) lies on a circle that intersects the circle $\mathbb{R} \cup \{\infty\}$ orthogonally. This concludes the proof.

(e) Show that for $z, w \in \mathbb{H}^2$, their hyperbolic distance $\mathrm{d}(z,w)$ satisfies

$$\mathrm{dist}(z,w) = \cosh^{-1}\left(1 + \frac{|z-w|^2}{2\mathrm{Im}(z)\mathrm{Im}(w)}\right)$$

Solution: If $z = ai$ and $w = bi$ like in the solution to the previous question, the formula we found for their distance coincides with the claimed formula.

Now suppose $z, w \in \mathbb{H}^2$ are generic points. Draw the geodesic through z and w and map it to the imaginary axis with an element $g \in \mathrm{PSL}(2,\mathbb{R})$. This allows us to compute their distance.

As a result, if we show that $\mathrm{d}(g(ai), g(bi))$ is indeed given by the formula above for all $a, b > 0$ and $g \in \mathrm{PSL}(2,\mathbb{R})$, we are done. This is a computation that is similar to the ones we've done above.

(f) Show that $g \in \mathrm{PSL}(2,\mathbb{R}) \setminus \{e\}$ acting on $\mathbb{H}^2 \cup \mathbb{R} \cup \{\infty\}$ has either one or two fixed points. Moreover, if g has two fixed points, they both lie on $\mathbb{R} \cup \{\infty\}$.

This leads to the following classification of elements $g \in \mathrm{PSL}(2,\mathbb{R}) \setminus \{e\}$

- g is called *elliptic* if it has a fixed point in $\mathbb{H}^2$
- g is called *parabolic* if it has a single fixed point in $\mathrm{R} \cup \{\infty\}$
- g is called *hyperbolic* (or *loxodromic*) if it has two fixed points in $\mathbb{R} \cup \{\infty\}$.

Show that g is elliptic, parabolic or hyperbolic if and only if it can be conjugated into $[K]$, $[N]$ or $[A] \subset \mathrm{PSL}(2,\mathbb{R})$ respectively. Finally, express the type of $g \in \mathrm{PSL}(2,\mathbb{R})$ in terms of $\mathrm{tr}(g)^2$.

Solution: $\overline{\mathbb{H}^2} = \mathbb{H}^2 \cup \mathbb{R} \cup \{\infty\}$ is a closed disk and $g : \overline{\mathbb{H}^2} \to \overline{\mathbb{H}^2}$ is a continuous function. By the Brouwer fixed point theorem, this implies g has at least one fixed point. g is also a Möbius transformation and hence uniquely determined by the image of three distinct points. So if g has at least three fixed points, it needs to be the identity. We conclude that g has either one or two fixed points on $\overline{\mathbb{H}^2}$.

Now, suppose g has two fixed points. If they both lie in $\mathbb{H}^2$, then, because g is an isometry of $\mathbb{H}^2$, g also fixes the unique geodesic segment between them setwise. But that means it must fix every point is this segment and hence that it's the identity. If only one of the points lies in $\mathbb{H}^2$ and the other in $\mathbb{R}^2 \cup \{\infty\}$, then g preserves the geodesic ray between these two points. This again means that it fixes every point on the geodesic ray (it can't translate along it, because it must fix the beginning) and thus that g is the identity.

To solve the second question, we observe that conjugating $g \in \mathrm{PSL}(2,\mathbb{R}) \setminus \{e\}$ does not change its type. Indeed, if we write $\mathrm{Fix}(g) \subset \overline{\mathbb{H}^2}$ for the fixed point set of g, we have $\mathrm{Fix}(hgh^{-1}) = h(\mathrm{Fix}(g))$.

Now if $g \in [K]$, it fixes i so it's elliptic. If $g \in [N]$ it fixes ∞, but no other point of $\mathbb{R} \cup \{\infty\}$ so it's parabolic and if $g \in A$, it fixes 0 and ∞.

Conversely, if g is elliptic, we can map its fixed point to i, which conjugates it into $[K]$. If g is parabolic we map its fixed point to ∞, thus conjugating it into $[N]$ and if g is hyperbolic, we map its fixed points to 0 and ∞, so that it cpnjugates into $[A]$.

Finally, the characterization of elements in terms of their trace can either be done using the Iwasawa decomposition again or by using the fixed point equation for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. The latter reads

$$\frac{az+b}{cz+d} = z \quad \Longrightarrow \quad az + b = cz^2 + dz$$

and thus

$$cz^2 + (d-a)z - b = 0.$$

The discriminant of this equation is

$$(d-a)^2 + 4bc = a^2 + d^2 - 2ad + 4bc = (a+d)^2 - 4 = \mathrm{tr}(g)^2 - 4$$

So: g is elliptic if and only if $\mathrm{tr}(g)^2 < 4$, parabolic if and only if $\mathrm{tr}(g)^2 = 4$ and hyperbolic if and only if $\mathrm{tr}(g)^2 > 4$.

(g) Show that the action of $G < \mathrm{PSL}(2,\mathbb{R})$ on $\mathbb{H}^2$ is properly discontinuous if and only if $G < \mathrm{PSL}(2,\mathbb{R})$ is discrete.

Solution: First suppose that G is not discrete. By Exercise 1(b), there mus exist a sequence $(g_n)_n$ of elements in G such that $g_n \to e$ as $n \to \infty$. Then $g_n(i) \to i$ as $n \to \infty$ (this for instance follows from the fact that the hyperbolic distance $\mathrm{d}(g_n(i), i)$ can be written explicitly in terms of the matrix coefficients of g_n, that are supposed to converge to those of the identity). This then means that if K is a compact set containing a closed disk around i, $g_n(K) \cap K \neq \emptyset$ for g_n large enough and hence contradicts proper discontinuity.

Now suppose that G is discrete. This means that it must be countable (G is a subgroup of a Lie group, so in particular a subset of a manifold). If we enumerate G,

$$G = \{g_1, g_2, \ldots\}$$

then the matrix norms $\|g_n\| \to \infty$ as $n \to \infty$. A computation yields that for any $g \in \mathrm{PSL}(2,\mathbb{R})$,

$$\|g\|^2 = 2\cosh(d(i, g(i))).$$

In particular $d(i, g_n(i)) \to \infty$ as $n \to \infty$. Now is $K \subset \mathbb{H}^2$ is compact, this means it's closed and contained in some closed (hyperbolic) disk around i. Since only finitely many g_n's keep K inside this ball, we get that the number of translates of K that intersect K itself is finite.

(h) Let

$$\begin{aligned}\Gamma(2) &:= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{Z});\ \begin{array}{ll} a \equiv d \equiv 1 & \mod 2 \\ b \equiv c \equiv 0 & \mod 2 \end{array} \right\} \\ &= \ker\left(\mathrm{PSL}(2,\mathbb{Z}) \overset{\text{reduction mod 2}}{\longrightarrow} \mathrm{PSL}(2,\mathbb{Z}/2\mathbb{Z})\right)\end{aligned}$$

Show that $\Gamma(2)\backslash\mathbb{H}^2$ is a Riemann surface.

Solution: Because all the matrices in $\Gamma(2)$ have coefficients in $\mathbb{Z}$, $\Gamma(2) < \mathrm{PSL}(2,\mathbb{R})$ is discrete. By Exercise 1(a), the only thing left to show is that $\Gamma(2)$ does not have any fixed points inside $\mathbb{H}^2$.

Suppose $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(2)$. By item (f), g has a fixed point in $\mathbb{H}^2$ if and only if

$$(a+d)^2 < 4.$$

So we would need, $a = -d$ or $a = -d+1$. We know that $1 \equiv a \equiv d \mod 2$. So we would need that $a = -d$. But then

$$ad = -a^2 = bc + 1 \equiv 1 \mod 4$$

However $a \mod 4 \in \{[1],[3]\}$ and

$$-1^2 \equiv -3^2 \equiv 3 \mod 4,$$

a contradiction.

Exercise 3 (Belyĭ maps). Suppose that X and Y are compact Riemann surfaces and $f : X \to Y$ is a non-constant holomorphic mapping. Recall that this implies that there exists a finite subset $C(f) \subset Y$ of *critical values* such that the cardinality $|f^{-1}(y)|$ is constant for $y \in Y \setminus C(f)$. The set $R(f) = Y \setminus C(f)$ is called the set of *regular values* of f. The cardinality of $|f^{-1}(y)|$ at a regular point $y \in R(f)$ is called the *degree* $\deg(f)$ of f. Note that $1 \leq |f^{-1}(y)| < \deg(f)$ for all $y \in C(f)$. Finally, recall that $x \in X$ is called a *regular* (resp. *critical*) point if $f'(x) \neq 0$ (resp. $f'(x) = 0$). The regular (resp. critical) values of f are exactly the images of the regular (resp. critical) points.

(a) Suppose that $X_1, \ldots, X_k$ are compact Riemann surfaces and suppose that $f_i : X_i \to X_{i+1}$ $(1 \le i \le k-1)$ is a sequence of non-constant holomorphic mappings. Set

$$f = f_{k-1} \circ \cdots \circ f_2 \circ f_1 : X_1 \to X_k.$$

Prove that $z \in C(f)$ if and only if there exists some $i \in \{1, \ldots, k-1\}$ such that the finite set $(f_{k-1} \circ \cdots \circ f_{i+1})^{-1}(z) \subset X_{i+1}$ contains a critical value for f_i.

Solution: First version: this is direct from the chain rule. Second version: a critical value of f is a point where f has fewer inverse images than usual, this must happen somewhere along the chain of compositions.

(b) A *Belyĭ map* is a holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$ that satisfies $C(f) \subset \{0, 1, \infty\}$. Show that the following maps are Belyĭ maps:

- The map $\beta_n : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ defined by $\beta_n(z) = z^n$.

  Solution: We write $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Moreover, we assume $n > 1$, if not the function does not have any critical points. In the chart $(\mathbb{C}, z \mapsto z)$, the derivative of β_n vanishes at 0 only. In the chart $(\mathbb{P}^1(\mathbb{C}), z \mapsto \frac{1}{z})$, the derivative vanishes at ∞. Conclusion $C(\beta_n) = \{0, \infty\}$.

- The map $\beta_{m,n} : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ defined by

  $$\beta_{m,n}(z) = \frac{(m+n)^{m+n}}{m^m n^n} z^m (1-z)^n.$$

  Where $m, n \in \mathbb{Z} \setminus \{0\}$ and $m + n \neq 0$.

  Solution: We have

  $$\beta'_{m,n}(z) = (m - (n+m)z) z^{m-1} (1-z)^{n-1}.$$

  which has a simple zero at $z = m/(m+n)$. Since $\beta_{m,n}\left(\frac{m}{m+n}\right) = 1$, we obtain that $1 \in C(\beta_{m,n})$. The other critical values are 0 (when $(m,n) \notin \{(1,1), (1,-2), (-2,1)\}$ and ∞ (when $(m,n) \notin \{(-1,-1), (-1,2), (2,-1)\}$.

- The map $\phi_d : \overline{X_d} \to \mathbb{P}^1(\mathbb{C})$ Defined as follows. Write $X_d = \{(x,y) \in \mathbb{C}^2;\ x^d + y^d = 1\}$, compactified by adding d points at ∞, corresponding to the d holomorphic branches of the d^{th} root. Define the projection map $\pi : X_d \to \mathbb{P}^1(\mathbb{C})$ by $\pi(x,y) = x$. Again, define $\beta_d : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ by $\beta_d(z) = z^d$. We set $\phi_d = \beta_d \circ \pi$.

  Solution: The critical values of π are the d^{th} roots of unity and ∞. β_d sends these to 1 and ∞ respectively, without creating new critical values.

(c) Now suppose

$$X = \overline{\{(x,y) \in \mathbb{C}^2;\ P(x,y) = 0\}}, \quad \text{with } P \in \overline{\mathbb{Q}}[x,y]$$

(and again the completion is performed by adding a suitable finite set of points at infinity)

- Show that there exists a branched covering $\pi : X \to \mathbb{P}^1(\mathbb{C})$ such that $C(\pi) \subset \mathbb{P}^1(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}} \cup \{\infty\}$.

  Solution: We can use the projection map $\pi : X \to \mathbb{P}^1(\mathbb{C})$ defined by $\pi(x, y) = x$ (and mapping the points at infinity to ∞). Indeed, by the holomorphic implicit function theorem, at the points
$$\left\{(x,y) \in X;\ \frac{\partial P}{\partial y}(x,y) \neq 0\right\}$$
  we can parametrize X holomorphically $x \mapsto (x, \varphi(x))$, where $\varphi : \mathbb{C} \to X$ is a local root of P in the second coordinate, that is, we have $P(x, \varphi(x)) = 0$. The composition $\pi \circ \varphi$ is the identity, which implies there are no critical points in this set.
  The remaining points are solutions to a system of polynomial equation with coefficients in $\overline{\mathbb{Q}}$, i.e.
$$P(x,y) = 0, \quad \frac{\partial P}{\partial y}(x,y) = 0.$$
  These two polynomials are relatively prime. Indeed, P is irreducible, so the only way they wouldn't be relatively prime is if P were to divide $\partial P/\partial y$, which is not possible because the latter has lower degree in y. This implies that their intersection has finitely many points with coordinates in $\overline{\mathbb{Q}}$. As such, the projection map π maps this set (containing all the critical points) into $\mathbb{P}^1(\overline{\mathbb{Q}})$.

- Since $C(\pi)$ is a finite set, we can assume (potentially by postcomposing with a Möbius transformation) that $\infty \notin C(\pi)$. Let f_1 be the minimal polynomial over $\mathbb{Q}$ of $C(\pi)$ – the monic polynomial of minimal degree that vanishes on all of $C(\pi)$. Construct the sequence of polynomials $f_2, f_3, \dots$ by letting f_{i+1} be the minimal polynomial over $\mathbb{Q}$ on the set
$$C(f_i) \cap \mathbb{C} = \{f(z) \in \mathbb{C};\ f_i'(z) = 0\}$$
  of finite critical values of f_i. Show that the degrees of these polynomials are strictly decreasing, that is: $\deg(f_{i+1}) < \deg(f_i)$ for $i \geq 1$.

  Solution: Our goal is to check that the degree of f_{i+1} does not exceed the number of finite critical points of f_i. Write $f_i' = \prod_j p_j$, where p_j are irreducible polynomials over $\mathbb{Q}$. Moreover, write $d_j = \deg(p_j)$. We have
$$\sum_j d_j = \deg(f_i) - 1.$$
  The roots of p_j form a complete set of conjugate algebraic numbers. Applying f_i (a rational polynomial) to these roots yields another complete set of conjugate algebraic numbers. The union of these sets of roots is exactly the set $C(f_i) \cap \mathbb{C}$ of finite critical values of f_i, which hence also forms a complete set of conjugate algebraic numbers.
  This implies that the minimal polynomial q_j over $\mathbb{Q}$ of the set of images of the roots of p_j has degree d_j. f_{i+1} is the product (without repetition) of these polynomials q_j. So
$$\deg(f_{i+1}) \leq \sum_j d_j < \deg(f_i).$$

- Since the degree is strictly decreasing, the sequence above terminates with a polynomial f_k of degree 1. Now set

$$f = f_k \circ \cdots \circ f_2 \circ f_1 \circ \pi : X \to \mathbb{P}^1(\mathbb{C}).$$

  Show that $C(f) \cap \mathbb{C} \subset \mathbb{Q}$.

  Solution: By (a),

$$C(f) \cap \mathbb{C} = \left((f_k \circ \cdots \circ f_1)\Big(C(\pi)\Big) \;\cup\; \bigcup_{j=2}^{k} (f_k \circ \cdots \circ f_j)\Big(C(f_{j-1})\Big) \right) \cap \mathbb{C}$$

  The polynomial f_{i+1} sends the finite critical values of f_i (or π) to 0. Moreover, $f_{i+2}, \ldots, f_k$ are rational polynomials, so the critical values stay in $\mathbb{Q}$.

- Show that if $|C(f)| \geq 4$, we can postcompose f with a holomorphic map $g : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ such that $C(g \circ f) \subset \mathbb{Q}$ and $|C(g \circ f)| < |C(f)|$. Conclude that we have proved that X admits a Belyĭ map.

  Solution: We first apply a Möbius transformation $g_0 \in \mathrm{PGL}(2, \mathbb{Q})$ such that $\{0, 1, \infty\} \subset C(g_0 \circ f) \subset \mathbb{Q} \cup \{\infty\}$. Because g_0 is an automorphism of $\mathbb{P}^1(\mathbb{C})$, it does not increase the number of critical values. Suppose that $z \in C(g_0 \circ f) \setminus \{0, 1, \infty\}$. We may write $z = m/(m+n)$ with $m, n \neq 0$ and $m + n \neq 0$. So we can set $g_1 = \beta_{m,n}$ from item (b). Indeed $C(g_1) \subset \{0, 1, \infty\}$, so it doesn't create any new critical values and moreover $g_1(z) = 1$. Again applying item (a), we get what we want. Since the procedure strictly decreases the number of critical values, we can repeat it until we've reached three critical values.

(d) Find Belyĭ maps on X_1, X_2, X_3 and X_4, given by:

$$X_1 = \{(x, y) \in \mathbb{C}^2;\ y^2 = x(x-1)(x-2/3)\}$$

$$X_2 = \{(x, y) \in \mathbb{C}^2;\ y^2 = (x-1)(x-\zeta_7)(x-\zeta_7^2)\} \quad \text{where } \zeta_7 = e^{2\pi i/7}$$

$$X_3 = \{(x, y) \in \mathbb{C}^2;\ y^2 = x(x-\zeta_7)(x-\zeta_7^2/\sqrt[7]{2})\} \quad \text{where } \zeta_7 = e^{2\pi i/7}$$

$$X_4 = \{(x, y) \in \mathbb{C}^2;\ y^2 = x(x+2)(x-\sqrt{31}+1)\} \cup \{\infty\}.$$

Remark: It's not so easy to find examples of curves defined of $\overline{\mathbb{Q}}$ but not $\mathbb{Q}$ for which the computation does not get out of hand. Don't hesitate to use your favorite computer algebra package to do some of the calculations.

Solution: The curves are listed in increasing order of computational difficulty.

For X_1 we apply the procedure from the proof above:

- The critical of the projection map $\pi : (x, y) \in X_1 \mapsto x \in \mathbb{P}^1(\mathbb{C})$ are $C(\pi) = \{0, 1, 2/3, \infty\}$. The finite critical values are already rational, so we can directly move on to the second stem of the process.

- The critical value we want to get rid of is $2/3 = 2/(2+1)$, so we use $\beta_{2,1}$. This means that a Belyĭ map on X_1 is given by

$$(x, y) \mapsto \beta_{2,1} \circ \pi(x, y) = \frac{27}{4} x^2 (1 - x).$$

For X_2:

- $\pi : (x, y) \in X_2 \mapsto x \in \mathbb{P}^1(\mathbb{C})$ are $C(\pi) = \{1, \zeta_7, \zeta_7^2, \infty\}$. The minimal polynomial f_1 of $\{1, \zeta_7, \zeta_7^2, \infty\}$ is $f_1(z) = z^7 - 1$
- $C(f_1) \cap \mathbb{C} = \{f_1(0)\} = \{-1\}$, so $C(f_1 \circ \pi) \cap \mathbb{C} = \{f_1(1), f_1(\zeta_7), f_1(\zeta_7^2), -1\} = \{0, -1\}$, which means that we can move on to the next step.
- Composing with the Möbius transformation $\beta : z \mapsto -z$, we obtain a map branched at $\{0, 1, \infty\}$, given by:

$$\beta \circ f_1 \circ \pi : (x, y) \mapsto 1 - x^7.$$

For X_3

- The critical values of the projection map $\pi : (x, y) \in X_2 \mapsto x \in \mathbb{P}^1(\mathbb{C})$ are $C(\pi) = \{0, \zeta_7, \zeta_7^2/\sqrt[7]{2}, \infty\}$. We could try to apply the procedure from the proof above again, but in this case there is a better functions to compose with. $\beta_7 : x \mapsto x^7$ maps the finite critical values directly into $\mathbb{Q}$, without creating any new ones. We have

$$\mathbb{C} \cap C(\beta_7 \circ \pi) = \left\{0, 1, \frac{1}{2}\right\}.$$

- Now we just need to get rid of $1/2 = 1/(1 + 1)$, so we apply $\beta_{1,1} : x \mapsto 4x(1 - x)$. This means that

$$(x, y) \mapsto \beta_{1,1} \circ \beta_7 \circ \pi(x, y) = 4x^7(1 - x^7)$$

is a Belyĭ map on X_2.

Finally, for X_4 we have:

- The critical values of the projection map $\pi : (x, y) \in X_3 \mapsto x \in \mathbb{P}^1(\mathbb{C})$ are $C(\pi) = \{0, 2, \infty, \sqrt{31} - 1\}$.
- The minimal polynomial of $C(\pi) \cap \mathbb{C}$ is

$$\begin{aligned} f_1(x) &= x(x + 2)(x - \sqrt{31} + 1)(x + \sqrt{31} + 1) \\ &= x(x + 2)(x^2 + 2x - 30) \\ &= x^4 + 4x^3 - 26x^2 - 60x \end{aligned}$$

so

$$\begin{aligned} f_1'(x) &= 4x^3 + 12x^2 - 52x - 60 \\ &= 4 \cdot (x^3 + 3x^2 - 13x - 15) \\ &= 4 \cdot (x + 1)(x - 3)(x + 5). \end{aligned}$$

So the finite critical values of f_1 are

$$C(f_1) \cap \mathbb{C} = \{f_1(-1), f_1(3), f_1(-5)\} = \{31, -225\}$$

because $f_1(3) = f_1(-5) = -225$. In particular, we're already in the situation that

$$C(f_1 \circ \pi) = \{0, 31, -225, \infty\} \subset \mathbb{Q},$$

so we don't need to construct f_2.

- We move on to the second step of the process: reducing the number of elements. First we pick a Möbius transformation $g_0 \in \mathrm{PGL}(2, \mathbb{Q})$ such that $g_0(0) = 0$, $g_0(\infty) = \infty$ and $g_0(31) = 1$, concretely
$$g_0(z) = z/31.$$
So $C(g_0 \circ f_1 \circ \pi) = \{0, 1\infty, -225/31\}$. We write
$$\frac{-225}{31} = \frac{-225}{-225 + 256}$$
and apply $\beta_{-225,256}$, given by
$$\beta_{-225,256}(z) = -\frac{31^{31} 225^{225}}{256^{256}} \frac{(1-z)^{256}}{z^{225}}.$$
So all in all, the Belyĭ map is given by
$$(x, y) \in X_3 \mapsto -\frac{225^{225}}{256^{256}} \frac{(x^4 + 4x^3 - 26x^2 - 60x - 31)^{256}}{(x^4 + 4x^3 - 26x^2 - 60x)^{225}} \in \mathbb{P}^1(\mathbb{C}).$$